VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Návrh procesu obnovy nekritických informačních služeb

Disaster Recovery Process Design of Non-critical Services

Student: Bc. Michaela Fusková

Vedoucí diplomové práce: Ing. Jan Ministr, Ph.D.

Ostrava 2012

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Michaela Fusková**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 1802T001 Aplikovaná informatika

Téma: Návrh procesu obnovy nekritických informačních služeb
Disaster Recovery Process Design of Non-critical Services

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska obnovy nekritických informačních služeb
3. Analýza současného stavu
4. Návrh procesu obnovy
5. Zhodnocení navrhovaného řešení
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

CARTLIDGE, Alison et al. *An Introductory Overview of ITIL® V3.* London: IT Service Management Forum, 2007. ISBN 0-9551245-8-1.
GREGORY, Peter. *IT Disaster Recovery Planning For Dummies.* Hoboken: Wiley, 2008. ISBN 978-0-470-03973-1.
SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích.* 3. rozšířené a aktualizované vyd. Praha: Grada, 2010. ISBN 978-80-247-3051-6.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Jan Ministr, Ph.D.**

Datum zadání: 25.11.2011
Datum odevzdání: 27.04.2012

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Čestné prohlášení:

„Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracovala samostatně“.

V Ostravě dne 25. 4. 2012 ……

Bc. Michaela Fusková

Obsah

Seznam pojmů

Seznam obrázků a tabulek

Seznam příloh

1. Úvod

Ve firmách, které jsou silně závislé na IT technologiích, může jejich narušení, trvající třeba jen několik málo hodin, vést k vážným finančním ztrátám a ohrožení přežití podniku. Pokračování činností takovéto organizace závisí na vedení, které by si mělo uvědomit, že zabývání se potencionálními katastrofami, které by mohly nastat, se v žádném případě nesmí brát na lehkou váhu. Nemělo by se také spoléhat na tvrzení, že to se nám přeci nemůže stát. Důležité zde je vypracovat plán, pro minimalizování narušení kritických i nekritických funkcí ve firmě. Proto by podniky měly začít čelit skutečnosti, že rizika nastat mohou a měly by se také naučit s nimi v případě, že se vyskytnou, pracovat. Musí se zde pamatovat, že rizika jednoduše nelze eliminovat či zcela odstranit, můžeme je však očekávat a naučit se je řídit. V organizaci existuje velké množství takovýchto rizik, která mohou představovat hrozbu – ať již větší, menší či zanedbatelnou. V žádném případě se však nesmí podceňovat. Proto je nutné určit priority z pohledu možného dopadu na činnosti v organizaci a pravděpodobnosti jejich výskytu.

Vhodný nástroj k minimalizaci hrozeb, které plynou z výskytu rizik, je zavedení plánu obnovy (disaster recovery plan, DRP). Jde o plán pro obnovu činností v organizaci po určité mimořádné události, který je součástí při zavádění systému řízení kontinuity činností (Business Continuity Management, BCM). Jde o novou problematiku, která se stává významnou v současném globálním světě podnikání plného neustálých změn, kde organizace existují. Pro maximální efektivitu se tento přístup musí stát součástí řízení společnosti. Výsledkem BCM je plán kontinuity činností, které tvoří zdokumentovaný soubor postupů a informací, které se udržují v neustále aktualizovaném stavu, připravených k použití v případě incidentu.

Cílem diplomové práce je zpracování návrhu metody obnovy pro informační systémy v reálné organizaci, které jsou nekritické. Chod těchto služeb se přímo netýká primární podnikatelské činnosti firmy, jako je například proces výroby výrobků, či poskytování služeb. Jde o služby týkající se například personalistiky nebo účetnictví. Jsou to služby, jejichž krátkodobý výpadek nezpůsobí firmě přerušení dodávek jejím zákazníkům. Úkolem práce je tedy analyzovat procesy ve firmě a ohodnotit možné hrozby, které mohou nastat. Dle hodnocení budou navrhnuta možná protiopatření, která dopad nepříznivé události zmírní.

2. Teoretická východiska práce, vymezení pojmů problémové oblasti

2.1 Použití ICT ve firmách

V dnešní době má rozvoj IT hlavní vliv na procesy v podnikání. Jedná se o technologie, jako jsou počítače, LAN, klient/server a v neposlední řadě také internet. Ty umožňují organizacím dodat jejich produkty a služby na trhy mnohem rychleji. Přenesli jsme se tím z průmyslové doby do doby informační. Vše se stalo mnohem rychlejší a dynamičtější. Tradičně orientovaná hierarchie v organizaci může být často komplikovaná vzhledem k neustále se měnícím trhům a to by mělo vést firmu k tomu, aby se stala více flexibilní. V průběhu tohoto bylo zapotřebí sjednotit a shrnout jednotlivé koncepty a postupy, které by umožnily lepší plánování, využívání a také zkvalitňování využitím informačních technologií, jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků nebo firem. Toto zapříčinilo vznik metodologie ITIL. (Commerce, 2005)

Při návrhu obnovy nekritických procesů ve firmě bude využit právě soubor konceptů a postupů ITIL. Bude se zde čerpat z knihy Service Delivery (zaměřující se na taktické procesy), kde se zaměříme na část, která se týká IT Service Continuity Managementu, tedy procesu řízení schopnosti poskytování určité úrovně služeb v případě výpadku systému. Z knihy Service Support (týkající se operativních procesů) se zaměříme na část Incident Management, která zajišťuje co nejrychlejší obnovení dodávky služby a minimalizaci důsledků výpadků služeb na firemní činnost.

2.1.1 Historie ITIL

Rané počátky ITILu se datují od roku 1982, kdy probíhají v britské vládě diskuze o efektivitě řízení ICT v jednotlivých vládních úřadech. Britská vláda si uvědomuje, že rapidně vzrostla závislost na ICT technologiích nejen ve firmách a jen málokterá organizace by dokázala fungovat bez této podpory. Tento vývoj zapříčinil nutný rozvoj této oblasti a také následné zvyšování kvality IT služeb a celkové infrastruktury. Tuto vzniklou situaci bylo proto třeba řešit. Britská vláda pověřila vládní agenturu CCTA[1] pro sestavení ucelené příručky, která by pomohla získat při řízení informatiky ve firmě přehled a kontrolu. Příručka měla být určená pro organizace prakticky jakéhokoliv zaměření (soukromé nebo vládní). CCTA oslovila manažery z různých společností a požádala je o sepsání zkušeností, které v jejich firmách byly dobře zvládnuty. Na základě těchto zkušeností byly sepsány postupy nejlepších zkušeností přímo z praxe, které CCTA vydala v roce 1989 dohromady ve 46

[1] CCTA – Central Computer and Telecommunications Agency

svazcích. Zde byly zkušenosti shrnuty a byl z nich vytvořen rámec, který lze aplikovat na jakoukoli společnost. ITIL se v té době stává závazným standardem pro management ICT služeb ve vládním sektoru. (HOSPES, 2005)

Dalším mezník v historii ITIL byl začátek 90. let. ITIL se u subdodavatelů[2] britské vlády osvědčil natolik, že i tito subdodavatelé začali po svých partnerech požadovat, aby zaručili svou stabilitu tím, že budou implementovat principy ITIL. V roce 1991 se také zakládá mezinárodní komunita IT Service Management Forum, která sdružuje profesionály i veřejnost zabývající se řízením ICT služeb. Díky tomu se také začaly rozvíjet praktické zkušenosti, znalosti a ITILu se začalo využívat ve stále více organizacích soukromého či veřejného sektoru. Ve druhé polovině 90. let se začíná pracovat na druhém vydání knihovny. Původně vydaných 46 svazků se přepracovává do komplexnějších knih. Základem jsou tituly Service Support a Service Delivery, které zahrnují podstatnou část ze všech svazků. Jsou vydávány také další knihy ITIL, které rozšiřují problematiku o oblasti, které jsou potřebné pro správné řízení informatiky ve firmách. ITIL se postupně celosvětově rozšiřuje a je považován za jakýsi mezinárodní standard pro oblast ITSM[3]. (HOSPES, 2005)

2.1.2 Definice ITIL

Za jednu z nejvýstižnějších definic lze považovat tuto: „ITIL je rozsáhlý, konzistentní a procesně orientovaný rámec pro řízení služeb informačních a komunikačních technologií založený na nejlepších zkušenostech z praxe“. ITIL je zkrácením názvu Information Technology Infrastructure Library. (SKÁLA, 2007)

2.1.3 ITIL v2, ITIL v3

V prvním vydání ITIL obsahoval 46 svazků a každý jeho díl byl vymezen pro jedenu dílčí část popisující řízení informatiky. Jistou nevýhodou zde byla absence větší provázanosti jednotlivých částí, ale ta byla odstraněna až v druhé části. Kromě tohoto tato verze také obsahuje přepracování změn za posledních deset let z důvodu neustálého vývoje informatiky (posun od mainframe systémů k aplikacím využívající klient-server přístup; rozvoj internetu). Na následujícím obrázku jsou uvedeny všechny součásti knihovny ITIL. Schéma nám také přibližuje vztahy publikací ITIL v2. Na jedné straně zde vidíme vztahy jednotlivých publikací k obchodním procesům a na straně druhé vztahy ICT infrastruktury. (SKÁLA, 2007)

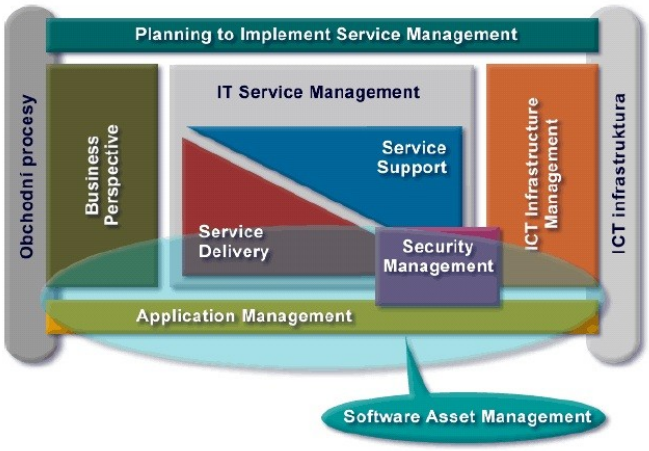
[2] Subdodavatel je podnik nebo organizace, která dodává jinému subjektu (podniku) dílčí dodávku pro jejich kompletaci.

[3] ITSM – IT service management

ITIL v2 nebyl skutečně ITILem v3 potlačen. Nové procesy, které se nachází v ITILu v3, jsou obsahem šesti ostatních knih ITILu V2. Tyto nové knihy jsou však procesně strukturované a proto i praktická vytíženost informací z těchto publikací je značně problematická. Nové procesy ITIL v3 vznikly dekompozicí procesů z verze předchozí a také proto nabízejí detailnější pohled na strukturu, obsah a rozsah popsaných procesů. (Itil, 2007)

V diplomové práci bude vycházeno z teorie uvedené v ITIL v2. Je to z toho důvodu, že ITIL v3 je zaměřen převážně na životní cyklus služeb, nikoli na jednotlivé složky ITSM.

Obr. 2.1: Schéma vztahů publikací ITIL v2



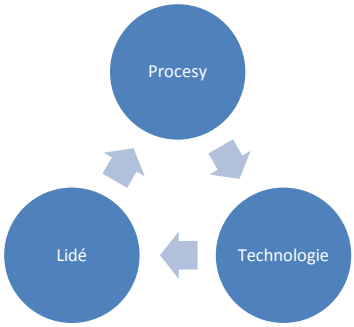
Zdroj: (SKÁLA, 2007)

2.2 Složky podnikání při návrhu postupu obnovy

Důležitá je zde souhra tří klíčových elementů, mezi které řadíme: lidi, procesy a technologie. Musí se zde brát v potaz důležitost souhry mezi těmito třemi elementy. Technologie jsou implementovány lidmi, kteří používají specifické procesy. Při navrhování procesů pro obnovu se musíme k těmto třem elementům neustále vracet. Bude zde potřeba lidi, kteří vědí, jak fungují procesy v organizaci a v jednotlivých odděleních. Tito lidé vědí kritická data, klíčové milníky a další informace, které jsou třeba při vytváření metodologie obnovy. Procesy při přístupu k obnově mají tyto dvě etapy: plánovací a implementační. Procesy, které v organizaci probíhají denně, se řadí mezi klíčové a jsou nezbytné k úspěšnému podnikání. Na druhou stranu zde existují také procesy, které nejsou kritické pro činnosti probíhající ve firmě, avšak jen do určitého časového intervalu. Když porovnáme například výpadek služby mzdového systému s výpadkem dodávky elektřiny, určitě je služba mzdového systému považována za méně kritickou. Musíme zde však brát v úvahu také načasování, tedy kdy k výpadku služby dojde. V našem případě by se jednalo o kritický problém, kdyby se

výpadek výplat mzdového systému stal těsně před výplatním dnem. Proto je zde nezbytné si jednotlivé procesy ohodnotit a vytvořit alternativní plány jak postupovat, když je určitá služba mimo provoz. Je nutné také vědět, co se děje s různými technickými komponentami během různých typů pohrom. Výpadek dodávky elektřiny například ovlivní všechnu technologii v budově. Je třeba vzít v úvahu ty technologie, které jsou potřebné v případě nouze – ty pro obnovu procesů, ale také ty pro zvládnutí krizové situace. (SNEDAKER, 2007)

Obr. 2.2: Vztah tří klíčových složek podnikání



Zdroj: (SNEDAKER, 2007)

2.2.1 Procesy, dělení procesů ve firmě

Proces značí opakovanou sekvenci činností, která generuje přidanou hodnotu[4]. Proces lze dále definovat jako transformaci vstupů na požadované výstupy. Jde o ekonomicky měřitelnou hodnotu produktu, je to činnost opakovatelná a pro zákazníka procesu jde o uspokojení jeho požadavku. Proces má jasně stanovené hranice – začátek a konec, včetně návazností na jiné procesy. Je zde také měřitelná výkonnost, jako je spotřeba zdrojů.

Procesy lze kvalifikovat do procesů hlavních a podpůrných. Hlavní procesy, nebo také klíčové (tvoří jádro byznysu), naplňují účel podnikání a vytváří přidanou hodnotu pro našeho zákazníka. Jedná se o sled činností, které leží na časově kritické cestě od požadavku zákazníka, až k uspokojení jeho potřeb a následnému zaplacení našeho produktu nebo služby zákazníkem. Naopak podpůrné procesy zajišťují vnitřnímu zákazníku, nebo našemu hlavnímu procesu, služby. Tyto služby je mnohdy možné zajistit i externě, avšak často se vykonávají přímo ve firmě – tedy interně. Externí i interní vykonávání má své výhody i nevýhody. U externího vykonávaní těchto služeb, tedy outsourcingu je určitě výhodou přenos rizika funkčnosti služeb na poskytující firmu. Možnou nevýhodou je únik důvěrných informací

[4] Proces nám vyjadřuje hodnotu, která je vytvořená díky procesům, při přeměně vstupů do výsledných výstupů (produktů nebo služby), kterou oceňuje zákazník procesu.

z firmy. Interní vykonávání je výhodné v tom, že právě my si vedeme to, co potřebujeme, a jak chceme, ale nevýhodou mohou být vyšší náklady na provoz těchto oddělení. Musíme tedy zvážit priority a rozhodnout, který ze způsobů provozování podpůrných služeb je pro nás ten nejvýhodnější. (BPM, 2003-2007)

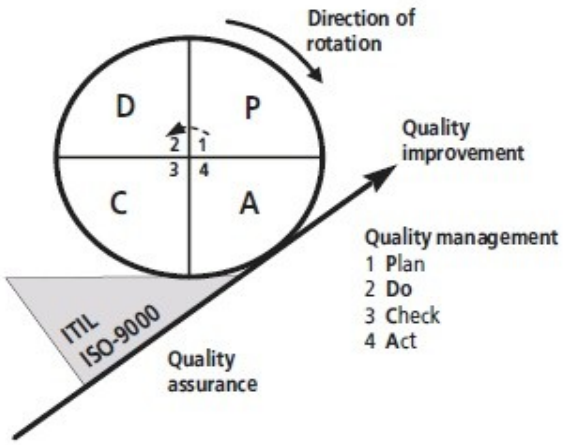
V diplomové práci se bude pracovat s procesy ve firmě, které jsou podpůrné tedy nekritické pro klíčový byznys probíhající ve firmě. V praktické části bude stanoveno, které procesy a s nimi související služby jsou konkrétně nekritické, a pro ně se pak v dalším kroku vytvoří návrh jejich obnovy.

2.3 Zajištění kvality

Dodávání produktů nebo služeb vyžaduje jisté aktivity. Kvalita produktu nebo služby závisí značně na způsobu, jakým jsou tyto aktivity organizovány. Demingův kruh kvality, který přibližuje následující obrázek, poskytuje jednoduchý a efektivní model pro kontrolu kvality. Model předpokládá, že k poskytnutí odpovídající kvality musí být opakovaně provedeny následující kroky:

- plánuj (plan): znamená co by mělo být uděláno, kdy by to mělo být uděláno, kdo by to měl provést, jak by to mělo být uděláno a za použití čeho,
- dělej (do): značí implementované naplánované aktivity,
- zkontroluj (check): stanovuje, jestli aktivity poskytuji odpovídající výsledky,
- jednej (act): přizpůsobí plány založené na nashromážděných informacích během kontroly. (Commerce, 2005)

Obr. 2.3: Demingův kruh kvality



Zdroj: (Commerce, 2005)

2.4 Service Level Agreement

SLA, se skládá ze slov: service, level a agreements (dále jen SLA). SLA definuje smlouvu o poskytování služeb, neboli jde o smlouvu o garantované úrovni služeb. Tento pojem vnikl díky potřebě co možná nejlépe definovat úroveň externě poskytovaných služeb, jejich rozsahu a opatření, proti možnému nedodržení předepsaných pravidel. Používá se hlavně v IT, kde je spojen s outsourcingem. Primárním účelem je zde definovat pravidla a případné sankce mezi dodavatelem a zákazníkem z pohledu poskytování služeb. Co se týče poskytování služeb v rámci outsourcingu, jedná se o jediný nástroj, díky kterému lze stanovit podmínky užívání služeb. SLA nám definuje, co je dodáno, v jaké kvalitě, kdy, za jakou cenu, míra zodpovědnosti a reakční časy v případě problémů. Díky tomuto zákazník dostane určitou jistotu, že obdrží funkcionalitu služeb takovou, za kterou zaplatil a v případě problémů bude provedena rychlá náprava. Součástí takovéto outsourcingované informační služby je však nejen programový balík na serveru, na němž je určitá aplikace provozována, ale také i komunikační infrastruktura a pracovní stanice, jejímž prostřednictvím se uživatelé ke svým datům dostávají. (SLA, 2011)

SLA se skládá ze tří částí:

Základní specifikace, podmínky a pravidla:

- kategorie příjemců,
- přesné vymezení počtu a umístění příjemců dané kategorie,
- popis služeb,
- objem poskytovaných služeb,
- bližší určení poskytovatele,
- měření (postup, způsob, periodicita, odpovědnost a vykazování výsledků),
- ověřování (postup, způsob, periodicita, odpovědnost),
- určení způsobu realizace podpory (fyzicky na místě, vzdáleně apod.),
- návazné podpůrné služby spojené s danou službou, například školení,
- cena služby,
- platební podmínky,
- pravidla pro změny služby,
- práva a povinnosti obou stran - podmínky součinnosti,
- ostatní podmínky pro realizaci SLA (bezpečnost, právo informovanosti, apod.). (Service, 2012)

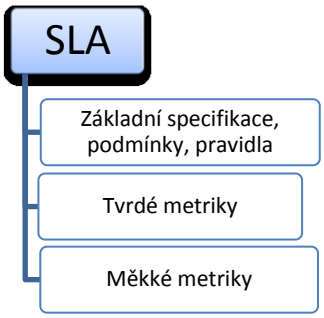
Tvrdé metriky:

- Dostupnost,
- běžná a maximální přípustná (kritická) doba odezvy na požadavek (incident),
- členění požadavků na jednotlivé typy, jako je hlášení poruchy aplikace, poruchy HW, přemístění koncové stanice, apod.). (Service, 2012)

Měkké metriky:

- ostatní metriky pro danou službu (kvalitativní ukazatele typu „potvrzení realizovaného školení a prezenční listina", „hodnocení lektora školení", „hodnocení účastníka školení", apod.). (Service, 2012)

Obr. 2.4: Části Service Level Agreement



Zdroj: (Service, 2012)

SLA definuje, jaké služby budou dodány, kdy (například časové rozmezí od 8:00 do17:00; čas do opravy nebo příjezdu technika) a kde (místo plnění služby). SLA také obsahuje postihy za případné nedodržení definovaných a námi požadovaných parametrů a někdy také pokutu za jejich překročení. Pro prokázání, nedodržení (nebo naopak překročení) stanovených parametrů slouží nástroje měření služby, požadavků a jejich vyřešení (k tomu slouží helpdesk). Hlavním cílem SLA je však dosažení vyšší uživatelské a zákaznické spokojenosti. Spokojenost uživatelů by měla být pro firmy, které tyto služby outsourcují jedním z nejdůležitějších faktorů. (Service, 2012)

2.5 Proces plánování, kroky při plánování procesu obnovy služeb

Je třeba si rozlišit dva pojmy, které bývají často zaměňovány, i přestože se jedná o zcela odlišné záležitosti. Business continuity planning (dále jen BCP) je metodologie, používaná pro vytváření a validaci plánu pro udržení kontinuity činností ve firmě před, během a také po havárii. Musí být zajištěn nepřetržitý chod základních funkcí a obnova funkcionality

všech systémů tak rychle, jak je to jen možné. Jedná se o koncept, který je používán pro ohodnocení různých technologických strategií ve firmách. V určitých firmách výpadek, který je obnoven do jisté doby, nevadí a nezpůsobí zas až tak kritické problémy. Existují však také společnosti, které si nemohou dovolit zcela žádný výpadek. Jedná se například o finanční instituce nebo transakce týkající se kreditních karet. Takovéto firmy musí zvážit, zda by náklady pro zajištění náhradního systému v případě výpadku byly výhodnou investicí, protože výpadek takovýchto služeb, a to třeba jen na pár minut, by mohl způsobit nemalé náklady a v určitých případech by třeba i mnohokrát předčil náklady na provoz záložního řešení. BCP se dívá dopředu a snaží se zmírnit důsledek nepříznivé události. Naproti tomu Disaster Recovery Plan (dále jen DRP) je plán navržený pro obnovu cílových systémů, služeb nebo počítačových zařízení v případě nouze. DRP se aplikuje na významné katastrofické události, díky kterým ztratíme přístup k běžným službám na určitou dobu. Cílem BC/DR plánování je pomoct předejít nástrahám, které mohou nastat a poskytnout zdravý, racionální a dobře promyšlený přístup ke zvládnutí pohromy, která nastala. (SNEDAKER, 2007)

Jsou zde také lidé, kteří mohou nastínit argument, že společnost může vynaložit nemalé finanční prostředky na naplánování něčeho, s čím se nikdy nebude muset vypořádat. Je to pravda, ale zkusme si to přirovnat k reálnému životu. Mnoho lidí řídí automobil celý svůj život a nestane se jim žádná autonehoda, ale pravděpodobně si i přesto platí pojištění. Výdaje na plánování musí být vyváženy mezi náklady na nedělání ničeho a mezi risk, který vyplývá z podnikání. Nakonec je tedy méně nákladné vynaložit příslušný čas a zdroje k vytvoření a udržení plánu, než v případě pohromy čelit situaci bez plánu. Nejde však vytvořit plán bez předchozího důkladného promyšlení, protože špatný plán nebo nekompletní je mnohem horší, než plán žádný. Nekompletní plány mohou vést lidi k chybám a mohou vést k mnohem většímu problému než samotná pohroma.

Pro plánování procesu obnovy služeb je zde ustanoveno několik základních kroků, které by se měly provést pro vytvoření spolehlivého plánu pro společnost. Tyto kroky zahrnují:

- zahájení projektu a výběr týmu,
- analýza dopadů na obchodní činnost (Business Impact Analysis, BIA),
- ohodnocení, analýza rizika (Risk Assesment, RA),
- strategie zmírnění vývoje (Mitigation Strategy Development),
- vývoj plánu (BC/DR plán), testování a audit,
- udržování plánu. (SNEDAKER, 2007)

Jako řada jiných projektů v IT, i BC/DR plánování musí mít definovaný start, průběh a konec. Tento průběh plánu pro obnovu je znázorněn na následujícím obrázku.

Obr. 2.5: Plánovací kroky BC/DR

Zdroj: (SNEDAKER, 2007)

2.5.1 Zahájení projektu a výběr týmu

Zahájení je jedna z nejdůležitějších oblastí při plánování obnovy, protože bez plně organizované podpory by byl plán jednoduše nekompletní. Nabízí se zde mnoho otázek, jako například: „Pokud bude server zničen a já mám nějaká záložní data, mám tím pádem také záložní server?“ nebo „Kde jsou uživatelé alokování?“ a další. Sami, jako autoři plánu obnovy, nebudeme schopni si bez podpory jednotlivých oddělení a divizí na tyto otázky odpovědět a proto je zde důležitá podpora právě od nich. Dosažení široké podpory lidí ze společnosti je pro plán obnovy klíčové, aby vůbec mohl uspět. (SNEDAKER, 2007)

2.5.2 Analýza dopadů na obchodní činnost

Jde o základ celého procesu řízení kontinuity činností organizace (BCM). Tvoří techniky a metody, díky kterým se hodnotí, jaké dopady by na organizaci a další zainteresované strany (zákazníky) mělo narušení dodávek jednotlivých služeb v organizaci a jejich podpůrných kritických činností. Součástí této analýzy je také stanovení minimálních úrovní zdrojů, které jsou potřebné pro obnovení jednotlivých činností ve stanovených časech a úrovních. (Commerce, 2005)

2.5.3 Ohodnocení rizika

Ohodnocení rizika znamená proces diskuze s klíčovými členy společnosti a analyzování potencionálních rizik, kterým společnost čelí. Riziko se zde objevuje od běžného až po mimořádné, tedy od požáru v několika místnostech, až po katastrofickou ztrátu, jako je například zemětřesení. Musíme zde definovat možný vliv vzniklých pohrom na technologické komponenty, ale samozřejmě to opět nezvládneme sami, tedy neobejdeme se bez podpory lidí z firmy. (STONEBURNER, 2002)

2.5.4 Strategie zmírnění rizika

Zmírnění je další z procesů řízení rizik, který nám stanovuje priority, hodnocení a implementuje vhodnou redukci. Záleží také, o jak velkou firmu se jedná. Pokud jsme v malé organizaci, může být strategie zmírnění docela jednoduchá: necháme si několik záložních kopií mimo firmu (nejlépe ve zcela jiné, avšak přístupné lokaci), včetně kopií klíčových informací jako je seznam zaměstnanců, telefonní čísla, seznam klíčových dodavatelů a našich zákazníků. Pro většinu společností je však proces mnohem složitější. Pro každé definované riziko, které má zpracováno analýzu dopadů, se musíme dívat na naše možnosti. Za jakých okolností může být riziko a dopad tolerovatelné, zredukované, případně jak se mu můžeme zcela vyhnout nebo ho přesunout? Tyto otázky se řeší v této části. (SNEDAKER, 2007)

2.5.5 Vývoj plánu

Po krocích analýzy se rovnou soustředíme na vývoj našeho plánu. Musí zde být zredukovány možné chyby a mezery. Měli bychom stanovit technické požadavky, zahrnout zde rámec pro rozpočet, harmonogram a hodnotová měřítka. (SNEDAKER, 2007)

2.5.6 Testování a audit

Když už je plán kompletní musíme lidi v organizaci zaškolit na implementaci. Je zde dobré si projít jednotlivé kroky, co dělat v případě pohromy, kdo za to bude zodpovědný a provést také simulaci takovéto události. Důležité je také plán otestovat a později i provést audit. (SNEDAKER, 2007)

2.5.7 Udržování plánu

Samotné udržování plánu je poslední z procesu plánování BC/DR. Plán by se měl obnovovat a kontrolovat, alespoň jednou za čas. Přece jenom se IT technologie a procesy ve firmě neustále vyvíjí a mění a právě tyto změny by měly být zaznamenávány také do plánu obnovy. (SNEDAKER, 2007)

2.6 Návrh procesu obnovy

Při návrhu obnovy jednotlivých služeb ve firmě bude vycházeno z již zmíněné teorie a ITILu. Naváže se na kroky, které byly nastíněny v předešlých kapitolách. Nejprve se začne s inicializací projektu, kde je hlavním účelem definování všech jeho parametrů, stanoví se příslušné kvalitní prostředí pro řízení, které je nezbytné pro úspěšné dokončení plánu obnovy. Jako první se bude vycházet z procesu analýzy činností organizace a dopadů, které mohou být způsobeny jejich narušením, tedy analýzy dopadů neboli Business Impact Analysis (dále

BIA). BIA je jakýmsi startovacím bodem pro identifikaci rizik pro zajištění kontinuity podnikání a může pomoci procesu Risk Assessment. V závěrečné fázi budou přiblíženy strategie zmírnění rizik, celkový vývoj plánu, testování, audit a průběžné udržování plánu.

2.6.1 Inicializace projektu

Při inicializaci projektu je třeba se podívat na jednotlivé kroky, které jsou nutné k zvládnutí BC plánu. Zaměříme se zde na řízení IT projektu (IT project management, IT PM). V příloze č. 1 je uveden návrh formuláře plánu činností projektu, včetně jejich časových rozvrhů, které jsou nutné při vytváření přesného časového plánu pro obnovu nekritických systémů. Obecně je třeba se také podívat na ty elementy, které jsou nutné pro úspěch projektu, zkontrolovat celkovou organizaci a v neposlední řadě také stanovit zodpovědný krizový tým.

2.6.1.1 Elementy úspěchu projektu

Je třeba si určit elementy, které pomohou k úspěšnému dokončení projektu. Jako první se musí určit zodpovědný vedoucí pracovník. Je logické, že podpora z top managementu organizace, je klíčová pro každý projekt. Díky tomu můžeme například získat potřebné finanční zdroje a zaměstnance. Důležitá je také účast zaměstnanců, kteří obsluhují jednotlivé služby a od nichž zjistíme potřebné informace o těchto službách, pro které bude tvořen návrh obnovy. Musí se definovat jasné a srozumitelné cíle projektu. Bez jejich definování se může stát, že bude věnováno příliš mnoho času méně důležité části plánu na úkor těm více důležitým. Dále je zapotřebí definovat požadavky projektu. Ty však nejsou to samé jako již zmiňované cíle projektu. Cíle by se měly řídit požadavky a jsou to ty, které chceme dokončit. Naproti tomu požadavky nám definují, jakým způsobem dosáhneme těchto cílů. (SNEDAKER, 2007)

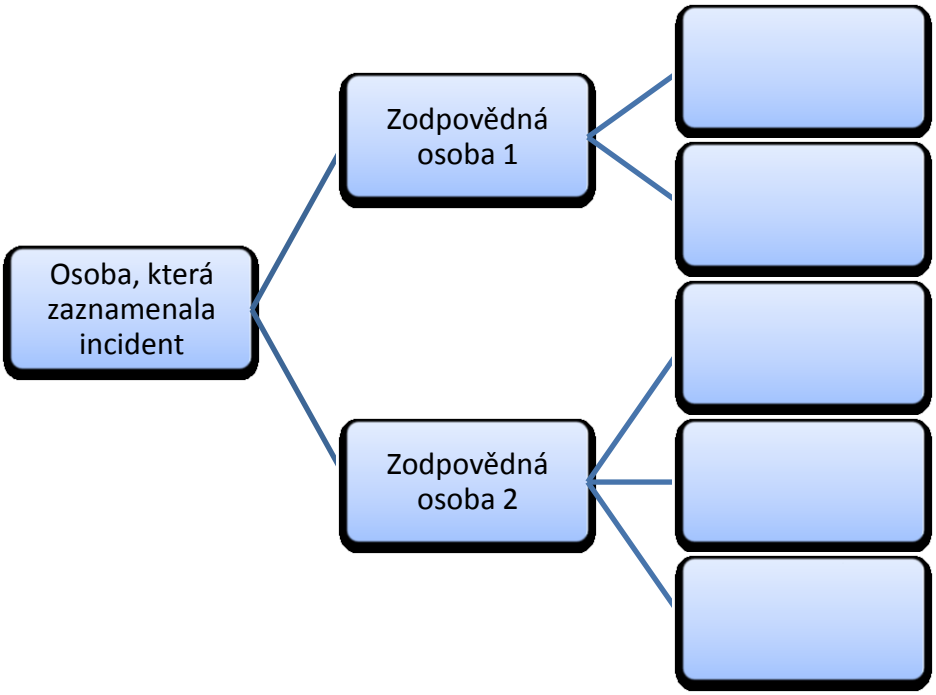
2.6.1.2 Organizace projektu, stanovení krizového týmu

Zde bude popisován postup implementace plánu pro obnovu nekritických služeb ve firmě. Celý systém zavádění plánu je veden tak, aby bylo pamatováno na neustále zlepšování, které je definováno cyklem PDCA (Plan-Do-Check-Act), a který byl již zmíněn v kapitole zabývající se teoretickými východisky.

Jako první by mělo být stanoveno, kdo bude členem krizového týmu firmy. Krizový tým je určité společenství zaměstnanců, které řeší krizové situace ve společnosti. Členové jsou vybíráni z konkrétních oblastí jako zástupci jednotlivých oddělení. Efektivita, s jakou bude případná krizová situace zvládnuta, primárně závisí na schopnostech jednotlivých členů týmu a díky tomu je třeba jmenovat odpovídající zaměstnance s dostatečnými pravomoci a

příslušnými schopnostmi k rozhodování. Členové krizového týmu by měli být nejlépe na manažerských pozicích nebo na pozicích nižších vedoucích. Je nutné mít v plánu obnovy zahrnuty kontaktní informace na tyto klíčové členy. Návrh formuláře je uveden v příloze č. 2. Kontaktní informace by měly být sepsány do přehledného seznamu a informace v něm uvedené by měly obsahovat také další kontakty od našich dodavatelů služeb. Formulář je uveden v příloze č. 3. Kromě kontaktních informací je třeba také stanovit hierarchii, komu je nutné volat v případě výskytu incidentu. Komunikační strom je vyobrazen na následujícím obrázku. (TECHTARGET, 2008-2012)

Obr. 2.6: Komunikační strom při vzniku incidentu



Zdroj: (TECHTARGET, 2008-2012)

Po úspěšné inicializaci projektu a nastínění jeho jednotlivých kroků se přistoupí k dalšímu kroku plánu obnovy nekritických informačních služeb.

2.6.2 Business impact analysis

Při tvorbě plánu obnovy musí být stanoveno, které činnosti ve firmě mají být analyzovány. Úkolem je zde vytvořit plán obnovy pro nekritické informační služby. Jde o takové, na kterých není přímo závislá činnost firmy a neovlivní tak přímo externího zákazníka. Výpadek takové služby je ale nekritický jen do určité doby. V tomto kroku bude nutné stanovit tyto služby, které jsou v organizaci nekritické a ohodnotit je vzhledem k dalším

kritériím. BIA odpovídá také na otázky typu: „Může být tato služba odložena (na jak dlouhou dobu)?“, „Může být funkce prováděna ručně?“ nebo „Jaký by byl efekt ztráty této služby na organizaci?“. Ideálním postupem k získání potřebných informací, je zde zaslat kopii formuláře BIA manažerům vybraných oddělení. Ti si jednotlivé kroky projdou a zodpoví otázky. Jednotlivé body je pak nejlépe probrat osobně přímo na schůzi s těmito lidmi z jednotlivých oddělení.

2.6.2.1 Faktory ovlivňující business impact analysis

Faktory business impact analysis (dále BIA), by měly zahrnovat různé metrické funkce týkající se podnikání jako je finanční dopad, reputace, lidé a potencionální výpadky. BIA nám pomáhá určit vzájemné závislosti mezi obchodními jednotkami (externími i interními) a závislostí v dodavatelském řetězci, minimální čas potřebný pro obnovu služeb a minimální počet zaměstnanců, kteří jsou schopni obnovit fungování služeb jako obvykle.

Dotazník BIA je důležitý, protože zjednoduší analýzu podnikání. Poskytuje jednotnost otázek a snadnost zapsání otázek do vhodného archivu jako je třeba tabulkový procesor. Tyto dotazníky mohou být také modifikovány vzhledem k adresovanému oddělení. Následující tabulka zobrazuje vztah mezi rušivou událostí a faktory podnikání, tedy základní otázku BIA. (KIRVAN, 2011)

Tab. 2.1: Vztah mezi rušivou událostí a faktory podnikání

Událost	**Napadená aktivita podnikání**	**Potencionální funkční ztráta**	**Potencionální finanční ztráta**	**Minimální čas potřebný pro obnovu služby**
Požár v datovém centru	Všechny aktivity v datovém centru	Nemožnost normálního fungování	Ztráta 60 000 Kč každou hodinu	3 – 5 hodin
Ztráta konkrétních zaměstnanců	Aktivity, které tyto zaměstnance potřebují	Redukuje možnost fungovat normálně	Ztráta žádná za předpokladu náhradního personálu	1 – 2 hodiny

Zdroj: (KIRVAN, 2011)

2.6.2.2 Otázky business impact analysis, tvorba dotazníku

Tyto otázky analyzují každou jednotku ve firmě, včetně IT. Otázky by se minimálně měly odpovídat na tyto záležitosti:

- porozumět jak každá služba ve firmě funguje,

- finanční hodnotu služby,
- závislosti na interním oddělení a podnikatelských jednotkách,
- závislost na externích organizacích,
- datové požadavky,
- minimální čas pro obnovu dat do původního stavu,
- minimální technologie a systémy potřebné pro provádění podnikání,
- minimální čas potřebný pro vrácení operací do normálního stavu po incidentu,
- minimální počet zaměstnanců potřebných pro provádění podnikání,
- minimum kancelářských prostor potřebných pro provádění podnikání,
- minimum kancelářských zařízení a služeb potřebných pro provádění podnikání.

Co se týče dotazníků, není dobré pokládat příliš mnoho otázek. Dobře organizovaná podnikatelská analýza by měla splnit rozsah od 20 do 25 otázek nebo i méně, pokud to je možné. V následující části jsou uvedeny některé startovní body, které by měla BIA zahrnovat.

- Definice podnikatelských procesů: Zde je třeba popsat procesy konkrétní podnikatelské jednotky. Uvést zde minimální časový rámec nutný pro obnovu podnikatelské jednotky a jejich specifických služeb (účetnictví) nebo aplikací (email).
- Závislost mezi podnikatelskými jednotkami a službami: Definují se zde podnikatelské jednotky, procesy a systémy, na jejíž provedení závisí podnikatelská jednotka či proces. Specifikuje se zde, zdali jsou tyto činnosti interní nebo externí vůči firmě, jako například dodavatelský řetězec.
- Určení kritičnosti procesů: Musí se zde určit, které z procesů jsou nekritičtější vzhledem k chodu organizace jako takové. Nejlepší je provést seřazení takovýchto služeb a přiřadit k nim jednotlivé priority.
- Dostupnost alternativních obchodních procesů, zaměstnanců a zdrojů: Specifikují se alternativní procedury jako například: ručně řešené objednávky nebo formuláře. Přístup k prozatímním zaměstnancům.
- Nahromadění práce: Určí se zde, jak dlouho potrvá vyřízení denních nedodělků práce za každý den výpadku.
- Maximální tolerance výpadku pro funkce, procesy, služby a systémy ve firmě: Určíme zde maximální množství času (hodiny, dny, týdny, měsíce), kdy obchodní jednotky, funkce, procesy, služby, systémy a zaměstnanci mohou být nedostupní předtím, než firmy ztratí podíly na trhu, výnosy či zákazníky.

- Stanovení vlivu vážnosti incidentu: Stanoví se zde kritičnost identifikovaného výpadku nebo narušení (nejhorší případ ohodnotím 5, událost bez vlivu 0).
- Stanovení vlivu na obchodní linii: Specifikujeme obchodní linii (výroba, účetnictví) a znovu vliv této události ohodnotíme (nejhorší případ ohodnotím 5, událost bez vlivu 0).
- Stanovení vlivu zásahu: Definuje a vyčísluje se vliv zásahu při nepříznivé události, jako je vliv na cash flow[5], konkurenční pozice, veřejná image, reputace či finanční reporty (nejhorší případ ohodnotím 5, událost bez vlivu 0).
- Finanční dopad: Vyhodnotím zde finanční dopad na mzdy, zisky, výdaje za určitá časová období jako jsou dny, týdny a měsíce.
- Minimálně přijatelný počet zaměstnanců: Specifikuje se zde minimální počet lidí potřebných pro každou podnikatelskou jednotku, aby byla schopna pracovat jako normálně nebo alespoň blízko normálu.
- Minimálně přijatelný počet konfigurovaných systémů: Jde o servery, routery[6], [7]switche, pracovní stanice, počítače, notebooky, telefony a kopírky.
- Minimální přijatelná dostupnost aplikací: Jedná se o operační systémy, databáze, aplikace potřebné pro zaměstnance k práci.
- Minimální přijatelné vybavení infrastrukturou: Stanovují se zde položky jako elektřina, hlasová a datová komunikace, dodávka vody a jídla.
- Minimální potřebný prostor pro zaměstnance.
- Minimální požadované pracovní pomůcky: Jde o nábytek, telefony, kancelářské zásoby.
- Definujeme unikátní nebo speciální požadavky: Zde záleží na konkrétní firmě, které z těchto požadavků bude potřebovat. Jde například o grafické stanice nebo specializované systémy. (KIRVAN, 2011)

[5] Cash flow je příjem nebo výdej peněžních prostředků. Představuje nám peněžní tok za určité období a představuje rozdíl mezi příjmy a výdaji peněžních prostředků za specifické období. Tato veličina vypovídá o schopnosti podniku generovat peníze.

[6] Router se používá v počítačové síti a jde o aktivní síťové zařízení, které procesem „routování“ přeposílá datagramy směrem k určenému cíli. To vše probíhá na třetí síťové vrstvě referenčního modelu ISO/OSI.

[7] Switch neboli přepínač je aktivní síťový prvek propojující jednotlivé segmenty sítě. Funguje na druhé datové vrstvě referenčního modelu ISO/OSI.

V další části BIA je vytvořen návrh formuláře, který poskytne analýzu vybraných nekritických služeb a určí vazby mezi jednotlivými procesy. Pro každou analyzovanou službu by měl být vyplněn formulář (přílohu č. 4).

2.6.3 Risk management, risk Assessment

Risk management popisuje metodologii řízení rizik včetně toho, jak toto řízení zapadá do každé fáze SDLC[8]. Risk management zahrnuje: risk assessment, risk mitigation (zmírnění rizika) a ohodnocení rizik. Společnosti implementují procesy řízení rizik do svých IT systémů právě z důvodu minimalizování negativního dopadu rizik na organizaci. Efektivní řízení rizik musí být plně integrováno do SDLC. SDLC IT systémů obsahuje pět fází vývoje: inicializace, vývoj nebo nákup, implementace, provozování s údržbou a odstranění. V některých případech se může IT systém nacházet v jednom časovém okamžiku ve více fázích. Řízení rizik je iterativní[9] proces, který může být prováděn během každé fáze SDLC. Následující tabulka popisuje charakteristiku jednotlivých fází SDLC a naznačuje, jaké řízení rizik by mělo být v jednotlivých fázích prováděno. (STONEBURNER, 2002)

Tab. 2.2: Charakteristiky fází SDLC, řízení rizik jednolitých fází

Fáze SDLC	Charakteristika fáze	Podpora aktivit risk managementu
Inicializace	Je zde vyjádřena potřeba IT systému. Účel a rámec IT systému je zdokumentován.	Identifikovaná rizika jsou používána pro podporu vývoje požadavků systému, zahrnující bezpečnostní požadavky.
Vývoj/nákup	IT systém je navrhnut, zakoupen nebo naprogramován.	Rizika identifikovány během této fáze mohou být použita pro podporu bezpečnostní analýzy IT systému. Díky tomu se zlepší struktura vývoje a celkové provedení IT systému.
Implementace	Prvky systémového zabezpečení by měly být nakonfigurovány, zpřístupněny, testovány a ověřeny.	Proces řízení rizik podporuje vyhodnocení systémové implementace s jejími požadavky.
Provozování a údržba	Systém provádí svou funkčnost, kvůli které byl pořízen. Typicky je systém neustále modifikován a to díky	Aktivity řízení rizik jsou prováděny pravidelně a i v případě jakékoli změny

[8] SDLC (System Development Lifecycle) je formalizovaný metodologický rámec pro vývoj informačních systémů.

[9] Iterativní, ve smyslu opakování procesu (latinsky iteretur – opakovat).

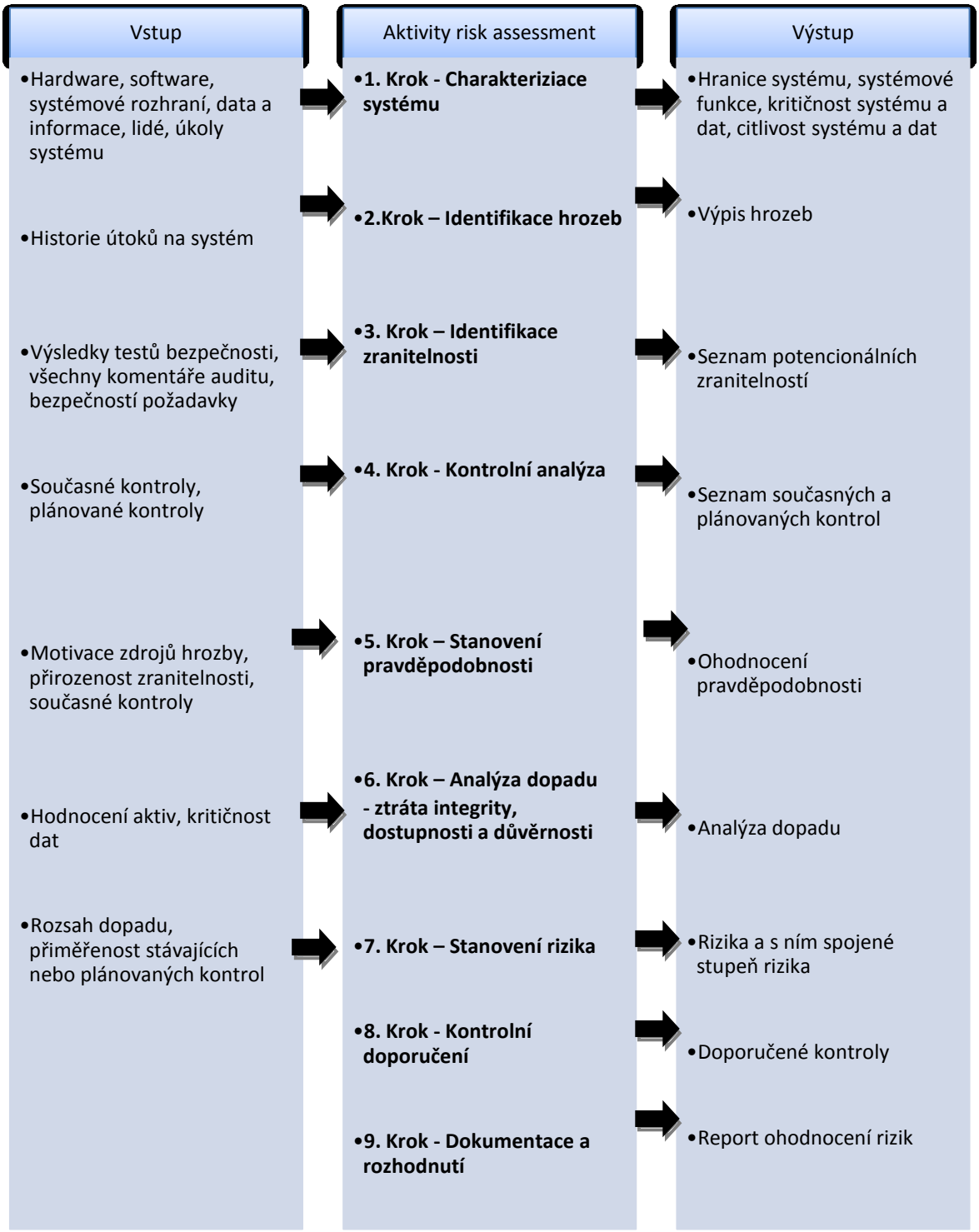
	změnám procesů organizace, politiky a procedur.	systému.
Odstranění systému	Tato fáze vyžaduje informace, hardware a software. Aktivity mohou zahrnovat přesun, archivaci, vyřazení nebo zničení systému.	Aktivity řízení rizik jsou prováděny pro systémové komponenty, které budou nahrazeny nebo odstraněny (například musí zde být proveden bezpečný přenos dat).

Zdroj: (STONEBURNER, 2002)

Řízení rizik je jakési řízení odpovědnosti. Toto řízení ve společnosti, jak již bylo dříve zmiňováno, má-li být úspěšné, musí být podporováno nejen vrcholovým managementem firmy, ale v neposlední řadě také uživateli systému.

Risk Assessment je první z procesů metodologie řízení rizik a zahrnuje identifikaci, ohodnocení rizik a dopad rizik i s doporučeními jak tato rizika redukovat. Organizace používají risk assessment ke stanovení rozsahu potencionální hrozby a rizika spojeného s IT systémem skrze své SDLC. Výstup tohoto procesu pomáhá identifikovat příslušné kontroly pro redukci nebo eliminaci rizika. Riziko je jakási funkce pravděpodobnosti, daná zdrojem hrozby, která využívá konkrétní zranitelnosti. Metodologie risk assessment se skládá z devíti doporučených kroků, které jsou popsány na následujícím obrázku a které vychází z procesní šablony CRAMM.

Obr. 2.7: Plánovací kroky risk assessment



Zdroj: (STONEBURNER, 2002)

2.6.3.1 Krok 1: Charakterizace systému

Nejprve je třeba v procesu risk assessmentu definovat rozsah, kterým se budeme zabývat. V tomto kroku je třeba definovat hranice IT systému společně se zdroji a informacemi, které představují systém. Díky tomu získáme potřebné informace například o hardwaru, softwaru, spojenosti systémů včetně přehledů zodpovědných divizí nebo pověřeném personálu. Tyto kroky jsou základní v oblasti definování rizik. Výstupem nám pak bude charakterizace IT systému, jeho vyhodnocení včetně vytvoření jakéhosi obrázku prostředí IT systému a popis systémových hranic.

V další části budou popsány informace, které se týkají systému a jeho prostředí. Dále bude vytvořen návrh technik, které jsou potřebné ke sběru příslušných informací.

Informace týkající se systémů

Identifikace rizik IT systému vyžaduje důkladné porozumění jeho procesům, které probíhají v systému a jeho prostředí. Zde je třeba nejprve shromáždit informace týkající se systému, které se vztahují k hardwaru, softwaru, rozhraní systému, jeho datům, informacím, personálu obsluhující a používající systém. Mezi další informace spojené s prostředím IT systému a jeho dat se dále zahrnují:

- funkční požadavky IT systému,
- uživatelé systému (systémoví uživatelé, kteří provádějí technickou podporu IT systémům; konečný uživatelé, kteří používají IT systém a jeho služby k provádění podnikatelských funkcí),
- politická řízení IT systému,
- architektura zabezpečení systému,
- současné topologie sítí,
- ochrany ukládání informací, které zabezpečí integritu dat a dostupnost dat,
- proud informací vztahující se k IT systému (systémové vstupy a výstupy),
- technické kontroly používané pro IT systém,
- kontroly managementu používané pro IT systém,
- operační kontroly IT systému,
- prostředí fyzického zabezpečení IT systému. (STONEBURNER, 2002)

Způsoby sběru informací

Pro sběr informací je nejlepší zvolit některou z následujících možností. Případně se používají i kombinace několika technik:

- dotazník: pro sběr relevantních informací, může být vytvořen dotazník týkající se managementu a operativních kontrol plánovaných nebo používaných v IT systému,
- interview probíhající na síti: interview s personálem, který podporuje a řídí IT systém. Interview poskytne dostatek informací o IT systému (například jak je systém řízen) i o specifikaci fyzického prostředí,
- přezkoumání dokumentace: zaměřuje se na politiku organizace a legislativu i se systémovou dokumentací (pro uživatele systému, manuál pro administrátory systému),
- použití automatického skenovacího nástroje: jde o aktivní technickou metodu používanou pro sběr informací (například síťový mapovací nástroj identifikuje služby, které běží na jednotlivých částech sítě). (STONEBURNER, 2002)

2.6.3.2 Krok 2: Identifikace hrozeb

Hrozba je potencionální zdroj, který může mít za následek poruchu systému a výpadek některé z jeho služeb. Musí zde být zahrnuty všechny možné zdroje hrozeb, které mohu způsobit poškození IT systému. Výstupem by měl být výčet jednotlivých hrozeb, který zahrnuje seznam zdrojů ohrožení, jež mohou narušit zranitelnost systému.

Typy pohrom, které se mohou objevit

Při tvorbě DR/BC plánu bychom se měli soustředit na pokrytí základů skrze všechny možné potencionální hrozby ve společnosti. Hrozby lze rozdělit do tří základních kategorií:

- přírodní hrozby,
- hrozby způsobené lidmi,
- nehody a technologické hrozby.

1. **Přírodní hrozby**

Přírodní hrozby jsou typy pohrom, které se nám vybaví nejdříve při uvažování o hrozbách. Vzpomeňme si jen například na ničivé zemětřesení a tsunami, které postihlo japonské Tokio v roce 2011 a mělo za následek ničivý dopad jak na celou infrastrukturu města, tak na jeho obyvatele. Nebo hurikán Katrina, který na konci srpna 2005 způsobil na jihu Spojených států nemalé škody. Musíme tedy pamatovat, že přírodní hrozby mohou být menší, významné nebo katastrofické, proto by plánování mělo zahrnovat tyto potencionální úrovně pohrom. Přírodní katastrofy mohou být očekávané nebo neočekávané. Například zmiňovaný hurikán Katrina byl neočekávaný a jeho následky byly devastující. Jednotlivé společnosti se ocitly v této situaci poněkud bezmocné, ale firmy, které měly zpracován plán

pro evakuaci, vzdálené zálohování dat a uložení, se postavily na své nohy dříve než ty firmy, které takovýto plán zpracovaný neměly.

V následující části je uveden stručný přehled pohrom, které nás mohou postihnout výskytem přírodních hrozeb:

Pohromy způsobné chladným počasím:

- laviny,
- sníh,
- ledová bouře,
- krupobití,
- dlouhotrvající vítr.

Katastrofy spojené s teplým počasím:

- dlouhotrvající déšť,
- záplavy,
- sucha,
- oheň (požár lesa, městský požár),
- tropické bouře,
- hurikány nebo cyklony,
- tornáda a větrné bouře.

Geologické pohromy:

- zemětřesení,
- tsunami,
- vulkanická erupce,
- sesuv půdy a posunutí půdy. (SNEDAKER, 2007)

Tento seznam pohrom není samozřejmě konečný, ale dává nám alespoň částečný výčet toho, co nás může postihnout. Musíme také pamatovat, že BC/DR plán by měl zahrnovat lidi působící napříč organizací a měl by brát v potaz různé lokace. Například máme-li kanceláře v Londýně, Peru a New Yorku, měli bychom pro každou lokaci, vzhledem k jejímu geografickému umístění, zpracovat specifický plán.

2. Hrozby způsobené lidmi

Tyto hrozby jsou poměrně odlišné než hrozby způsobené přírodou a většina z nich je úmyslných. Mezi tyto hrozby řadíme:

- terorizmus (bomby, ozbrojené útoky, biologický útok, útok při transportu, útok na infrastrukturu, únosy),
- exploze,
- oheň (žhářství nebo neúmyslný požár),
- kybernetický útok (menší vniknutí, větší vniknutí, totální výpadek, neautorizované použití hesel a klíčů, zneužití dat, rozhněvaní zaměstnanci, neúmyslné přestupky, DoS útok[10], viry a červi, trojské koně),
- civilní nepokoje a neklid,
- protesty,
- kontaminace radioaktivitou,
- vydírání,
- vnitřní politika (sabotáže našich zaměstnanců). (SNEDAKER, 2007)

3. Nehody a technologické hrozby

Tyto nehody a technologické hrozby jsou často zapříčiněny pohromami způsobenými člověkem a liší se v tom, že jsou většinou neúmyslné. Jsou to:

- transportní pohromy a selhání (letištní kolaps, železniční kolaps nebo nehoda, potrubní kolaps),
- pohromy infrastruktury (dodávka elektřiny, plynu, vody),
- infrastruktura informačních systémů (výpadek internetu, přerušení komunikační infrastruktury jako jsou podvodní kabely, satelity, výpadek hlavního poskytovatele internetu, selhání systémů),
- selhání rozvodné sítě a elektřiny,
- selhání nukleárního zařízení,
- pohromy s hazardním materiálem (místní nebo stojící zdroj, nelokální či přepravní zdroj jako je havárie nákladního auta, které táhne radioaktivní nebo chemický odpad),
- kolaps budovy (z různých příčin). (SNEDAKER, 2007)

Pro minimalizování těchto možných incidentů je potřebné mít zpracován spolehlivý plán, který je také opakovaně testován a obnovován.

2.6.3.3 Krok 3: Identifikace zranitelnosti systému

Cílem tohoto kroku je vytvoření seznamu zranitelností systému (slabé stránky, chyby, nedostatky). Jednou z metod pro identifikaci systémové zranitelnosti je použití jejich zdrojů,

[10] DoS útok znamená záplavu protokolem ICMP, surf útok, ping smrti.

provedení testování zabezpečení systému a vývoj seznamu bezpečnostních požadavků. Výstupem tohoto kroku by měl být seznam zranitelnosti systému, které mohou být využívány potencionálními zdroji hrozeb. (SNEDAKER, 2007)

2.6.3.4 Krok 4 : Kontrolní analýza

Má za cíl stanovit seznam současných nebo plánovaných kontrol používaných pro IT systémy pro zmírnění rizika pravděpodobnosti zranitelnosti. Díky tomu, že je řízeno je redukován jeho vliv na nepříznivou událost. (SNEDAKER, 2007)

2.6.3.5 Krok 5: Stanovení pravděpodobnosti

Zde se ohodnotí pravděpodobnosti výskytu nepříznivé události. Musíme brát v potaz motivaci zdrojů nepříznivé události včetně jeho schopností, vlastnost zranitelnosti existence a efektivitu současných kontrol. Pravděpodobnost, že potencionální zranitelnost by mohla být využita zdrojem hrozby lze popsat jako vysokou, střední a nízkou. Definice pravděpodobností jsou uvedeny v následující tabulce. (STONEBURNER, 2002)

Tab. 2.3: Definice pravděpodobností

Stupeň pravděpodobnosti	Definice pravděpodobnosti
Vysoká	Zdroj je vysoce motivovaný a schopný a preventivní kontroly jsou mnohdy neefektivní a neúplné.
Střední	Zdroj hrozby je motivovaný a schopný, ale kontroly mohou pomoci zabránit výpadku.
Nízká	Zdroj hrozby nemá dostatek motivace nebo schopnosti anebo kontroly jsou natolik preventivní, že je velmi nízká pravděpodobnost výpadku služby.

Zdroj: (STONEBURNER, 2002)

2.6.3.6 Krok 6: Analýza dopadu

Dalším důležitým krokem při měření úrovně rizika je určení nepříznivého dopadu. Před zahájením této analýzy je však nutné získat tyto informace týkající se:

- účelu a cílů systému,
- kritičnosti systému a jeho dat (hodnota určitého systému a jaký má význam pro organizaci),
- citlivosti systému a dat.

Tyto informace lze získat z existující dokumentace organizace, jde o business impact analysis. Upřednostňuje vliv dopadu spojený s kompromisem organizace, který je založený na

kvalitativním a kvantitativním ohodnocení citlivosti a kritičnosti každého aktiva. Proto by se mělo při posuzování dopadu nepříznivé události vycházet z následujících tří bezpečnostních cílů: integrity, dostupnosti a důvěrnosti. V následujícím seznamu je popis jednotlivých bezpečnostních cílů a jejich důsledků:

- Ztráta integrity znamená, že systém a integrita dat se odkazuje na požadavek, aby byly informace chráněny před nevhodnými modifikacemi. Integrita je ztracena, pokud jsou prováděny neoprávněné změny údajů. Další používání těchto dat může mít za následek nepřesnosti a může zapříčinit chybná rozhodnutí. Také porušení integrity může být prvním krokem k úspěšnému útoku na dostupnost a důvěryhodnost systému. Ze všech těchto důvodů ztráta integrity znamená redukci zabezpečení konkrétního IT systému.
- Ztráta dostupnosti. Pokud posuzovaný IT systém a jeho služby nejsou dostupné svým uživatelům, pak poslání organizace mohou být negativně ovlivněny. Provozní efektivita například může vést ke ztrátě produktivního času a tak brání výkonu práce koncovým uživatelům v provádění cílů organizace a celkově podnikání firmy.
- Ztráta důvěryhodnosti. Systém a důvěryhodnost dat, se vztahují, na ochranu před neoprávněným zveřejněním. Takový dopad neoprávněného zveřejnění důvěrné informace se může pohybovat od ohrožení národní bezpečnosti ke zveřejnění soukromých nebo osobních dat. Neautorizované, neúmyslné nebo neočekávané zveřejnění by mohlo vést ke ztrátě důvěry nebo i soudnímu postihu vůči organizaci. (STONEBURNER, 2002)

Některé dopady lze měřit kvantitativně jako je ušlý zisk, náklady na opravu systému a zprovoznění jednotlivých služeb nebo úrovní úsilí k nápravě problémů, které jsou způsobeny působením hrozeb. Ostatní vlivy, mezi které řadíme například ztrátu důvěryhodnosti veřejnosti, nelze měřit v měrných jednotkách, ale lze je kvalifikovat jako vysoké, střední a nízké dopady. V následující tabulce jsou popsány právě kvalitativní kategorie dopadů na jednotlivé IT služby. (STONEBURNER, 2002)

Tab. 2.4: Kvalitativní kategorie dopadů na IT službu

Rozsah dopadu	Definice dopadu
Vysoký	Výskyt této chyby zabezpečení může vést k velmi nákladné ztrátě na hmotném majetku nebo zdrojích, které může výrazně porušit fungování firemních procesů a brání organizaci v jejím poslání, kazí pověst a v některých případech může mít za následek dokonce i vážné zranění lidí.
Střední	Výskyt této chyby v zabezpečení může mít za následek nákladné ztráty na hmotném majetku a ostatních zdrojích. Porušuje a brání organizaci v plnění svých cílů a může mít za následek i zranění lidí.
Nízký	Tato chyba v zabezpečení vede ke ztrátě hmotného majetku nebo zdroje. Ovlivňuje pověst organizace.

Zdroj: (STONEBURNER, 2002)

Při provádění analýzy dopadů by se však měly vzít v úvahu výhody a nevýhody srovnávání s kvalitativním a kvantitativním hodnocením. Výhodou kvalitativní analýzy dopadu je to, že upřednostňuje rizika a určuje oblasti pro okamžité zlepšení v řešení zranitelnosti. Naproti tomu její nevýhodou je to, že neposkytuje konkrétní měřitelné velikosti dopadů. Pro kompletní analýzu dopadů tedy musíme ještě posoudit další z těchto faktorů:

- odhad frekvence zdroje hrozby při výkonu této chyby na určitou dobu (například 1 rok),
- orientační náklady na každý výskyt nepříznivé události. (STONEBURNER, 2002)

2.6.3.7 Krok7: Stanovení rizika

Účelem tohoto kroku je posouzení stupně rizika IT systému. Pro měření rizika je nutné vytvořit měřítko a matici stupně rizika. Ta popisuje konečné stanovení rizika vynásobením hodnoty přidělené pro ohrožení pravděpodobnosti a hrozby dopadu. Na následující stránce uvádím matici 3 x 3, kde pravděpodobnosti hrozby je vysoká, střední nebo nízká a ohodnocují se 1,0 pro vysokou, 0,5 pro střední a 0,1 pro nízkou. Dopad hrozby je také vysoký, střední, nízký a ohodnocení je 100 pro vysoký, 50 pro střední a 10 pro nízký. (STONEBURNER, 2002)

Tab. 2.5: Matice stupně rizika

Pravděpodobnost hrozby	Dopad		
	Nízký (10)	**Střední (50)**	**Vysoký (100)**
Vysoký (1,0)	Nízké 10 X 1,0 = 10	Střední 50 X 1,0 = 50	Vysoký 100 X 1,0 = 100
Střední (0,5)	Nízké 10 X 0,5 = 5	Střední 50 X 0,5 = 25	Střední 100 X 0,5 = 50
Nízký (0,1)	Nízké 10 X 0,1 = 1	Nízké 50 X 0,1 = 5	Nízké 100 X 0,1 = 10

Měřítko rizika: Vysoké (>50 do 100); Střední (>10 do 50); Nízké (1 do 10)

Zdroj: (STONEBURNER, 2002)

a) Analýza rizik: kvalitativní a kvantitativní metoda

Jde o způsob vyjádření veličin, s kterými se v analýze rizik pracuje. Existují dva základní přístupy k řešení: kvalitativní a kvantitativní. Je zde možné použít buď jeden přístup anebo kombinaci více přístupů kvalitativní a kvantitativní metody.

Kvalitativní metody

Rizika se zde definují tak, že stanovena v určitém přesně daném rozsahu (příklad obodování <1 až 10>; pravděpodobnost <0;1>; slovně). Výhodou je, že jsou jednodušší, rychlejší, ale více subjektivní. Nesou však problémy v posuzování přijatelnosti finančních nákladů potřebných k eliminaci hrozby – ta může být charakterizována jako „velká až kritická“. V důsledku toho nám pak chybí jednoznačné finanční vyjádření a efektivnost nákladů se znesnadňuje. (SMEJKAL, 2010)

Kvantitativní metody

Ty jsou založeny na matematickém výpočtu rizika frekvence výskytu hrozeb a jejího dopadu. Zde se již vyjadřuje dopad ve finančních termínech (například tisíce Kč; riziko je vyjádřeno formou roční předpokládané ztráty, anglicky Annualized Loss Expectancy – ALE). Tyto metody jsou založeny spíše na přesnosti, než na kvalitě. Zpracování za pomocí metod také vyžaduje více času a úsilí, odměnou je však přesné vyjádření rizik. Nevýhodou kromě složitosti však může být vysoce formalizovaný postup, který v krajním případě vede k opomenutí posouzení specifik subjektu, a to pak může vést k jeho vyšší zranitelnosti. A to

z důvodu zahlcení hodnotitele velkým objemem formálně strukturovaných dat. (SMEJKAL, 2010)

b) Volba strategie analýzy rizik: delphi, CRAMM

Lze využít čtyř hlavních přístupů: základní, neformální, podrobná analýza rizik a kombinovaný přístup. Vhodnou analýzu rizik vybíráme ve dvou krocích. Orientační analýza klíčových rizik slouží pro následné rozhodování o volbě konkrétní metody. Pro tyto objekty je pak v dalším kroku provedena detailní analýza všech možných rizik některou z metod (kvalitativní, kvantitativní). Nejlepší je kombinace metod, jde však o nejnákladnější a nejdelší způsob. Rozhodnutí, který přístup je pro daný objekt vhodný závisí hlavně na následujících skutečnostech:

- jakých cílů má být použitím analýzy rizik dosaženo,
- k jakým účelům objekt slouží,
- jaká je hodnota aktiv spojených s objektem,
- zda jsou funkce, které objekt poskytuje kritické a pro koho,
- jaká je úroveň investic do objektu a jaká je výše nákladů na obnovení jeho funkčnosti. (SMEJKAL, 2010)

Kvalitativní metoda: Metoda účelových interview (metoda Delphi)

Při kvalitativní analýze rizik se používá metoda účelových interview (metoda Delphi). Zde se používá pro rizikovou analýzu soubor otázek, prodiskutovaných na účelových pohovorech. Otázky jsou většinou tvořeny dvěma částmi – pevnou (předem danou) a variabilní (dle průběhu pohovoru a postavení respondenta). Respondenti nepřicházejí při zpracování odpovědí do styku kvůli vyvarování se možného ovlivňování. Výhodou je menší náročnost na čas a spotřebu zdrojů. Tato metoda se používá hlavně z důvodu, že nám určuje, co se může stát a za jakých podmínek. (SMEJKAL, 2010)

Nevýhodou je absence jednoznačného finančního vyjádření, která je však kompenzována začleněním tohoto kritéria do pohovorů, které (pokud se jedná o úplnou variantu metody Delphi) probíhají iteračně. Tedy výsledky z jednoho kola rozhovorů jsou po statistickém zpracování sděleny respondentům, kteří jsou pak vyzváni k zaujetí jednoznačného stanoviska, kdy mají možnost korigovat anebo naopak zdůraznit původní stanoviska (doporučuje se provedení 2 až 3 iterací). Existují také různé subvarianty (metoda anketní analýzy, scénářů, matic). (SMEJKAL, 2010)

Kvantitativní metody: CRAMM

Využívané především v oblasti bezpečnosti organizací a jejich IS. Metodika CRAMM byla vyvinuta pro potřeby vlády Velké Británie. Dnes je široce využíván jako prostředek pro analýzu rizik v případech, kdy je vyžadován souhlas s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799. Analýza CRAMM řeší ohodnocení systémových aktiv, dále seskupení aktiv do logických skupin a stanovení hrozeb, které působí na tyto skupiny, prozkoumání zranitelnosti systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny. Poté jsou navrhnuta bezpečnostní opatření, která jsou vymezena ve shodě s úrovní rizika při porovnání s již implementovanými systémovými opatřeními.

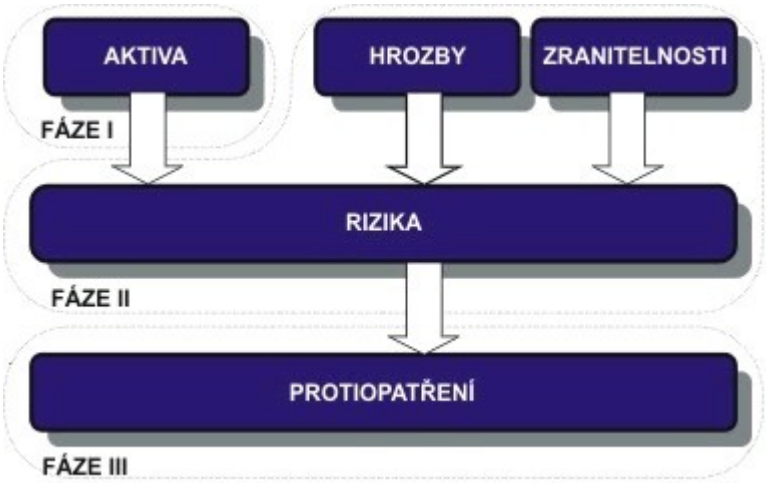
c) Návrh tabulky pro konkrétní řešení risk assessment metodou CRAMM

V následujícím postupu bude popsána realizace návrhu konkrétní tabulky pro řešení risk assessment metodou CRAMM. Nejprve však je přiblížena problematika CRAMM s definicí o co vlastně jde a co díky ní může být analyzováno.

CRAMM

Jde o procesní šablonu pro analýzu rizik a pro zvládnutí těchto rizik skrz protiopatření. Existuje také mnoho druhů softwaru pro podporu CRAMM. Bude však vycházeno z manuální techniky CRAMM. CRAMM nám poskytuje jakýsi rámec pro kalkulaci rizik. Analýza a řízení rizik za pomoci CRAMM probíhá ve třech fázích: identifikace včetně hodnocení aktiv, analýza hrozeb a zranitelnosti a řízení rizik. Jednotlivé fáze jsou zakresleny na následujícím obrázku. (CRAMM, 2012)

Obr. 2.8: Fáze CRAMM



Zdroj: (CRAMM, 2012)

CRAMM zahrnuje tento pevný formát:

- používá porady, interview a dotazníky pro sběr dat,
- identifikuje a kategorizuje IT aktiva do těchto tří kategorií: data, aplikace/software a fyzická aktiva (budovy, vybavení, zaměstnanci),
- požaduje uvážení dopadu na ztrátu důvěrnosti, integrity a dostupnosti aktiv,
- vyjadřuje zranitelnost (pravděpodobnost, že hrozba může nastat) jako: velmi vysokou, vysokou, střední, nízkou nebo velmi nízkou,
- vyjadřuje riziko (pravděpodobnost, že hrozba by mohla narušit zranitelnost) jako: vysokou, střední nebo nízkou. (SMEJKAL, 2010)

Zde je třeba získat příslušnou autoritu pro získání přístupu k zabezpečení jednotlivých služeb. Dále se musí vymezit rozsah přezkoumání (definují se jednotlivé IT služby, umístění, aplikace), přidělí se tým a identifikují se zdroje informací. Vymezí se návrh recenze a konkrétně se specifikuje řízení projektové dokumentace. Tedy až teď jsme připraveni začít s první fází a ta se zabývá identifikací aktiv v rámci rozsahu přezkoumávaných dat (zde v rámci nekritických informačních služeb). Lze využít i dřívější Business Impact Analysis (BIA). Dále je připraven návrh tabulky, ve které je důležité to, že každý majetek nebo seznamu majetků má svého vlastníka. Vlastník je osoba, která ví nejlépe, jak použít toto aktivum a také jaká je jeho hodnota. Dále je na řadě rozhovor s vlastníkem aktiva. Vlastník aktiva by měl ohodnotit data a software z hlediska dopadu nebo nákladů v případě ztráty

důvěrnosti, integrity a dostupnosti. Také se musí ohodnotit náklady při případné náhradě aktiv. Vlastníci se musí zaměřit na následující atributy a jejich aktiva:

- Důvěrnost znamená vliv nebo náchylnost ke zveřejnění majetku neautorizovaným osobám (například jde o data a údaje o zaměstnancích, smluvních stranách apod.) Zde je použita kategorizace důvěrnosti jako: veřejná (0), omezená (1-5), důvěrná (6-9), zabezpečená (10).
- Integrita vyjadřuje vliv neznámé nebo neautorizované úpravy (například chyby ve vstupních datech). Pro kategorizaci integrity je použita stupnici hodnocení: nízká (1-3), přiměřená (4-6), vysoká (7-9) a velmi vysoká (10).
- Dostupnost znázorňuje vliv aktiva v případě nedostupnosti po různé časové rámce (například méně než 15 minut, 1 hodinu, 1 den). K této kategorizaci je navrhnuta stupnice: nízká (1-3), přiměřená (4-7), vysoká (8-9), velmi vysoká (10). (Marquis, 2012)

Nejprve by se měla analyzovat důvěrnost a dostupnost. Vlastník nebo zodpovědné osoby by si měly vybrat nejprve z kategorie hodnocení. Například pro integritu, se zvolí hodnocení mezi nízkou, přiměřenou, vysokou a velmi vysokou. Pokud se zde bude rozhodnuto ohodnocení integrity jako přiměřené, měl by se dopad hodnotit na měřítku od 4 do 6.

V další částí se zjistí, jaká je pravděpodobnost hrozby. Je třeba klást otázky obsluhujícímu personálu, expertům nebo dalším zainteresovaným zaměstnancům použitím připraveného dotazníku. Tím si vyzkoušíme a zhodnotíme pravděpodobnost, že by zjištěná rizika mohla skutečně nastat. V konkrétním případě se hodnotí hackeři (uvnitř i vně společnosti), viry nebo poruchy (ať už hardwaru nebo softwaru), pohromy (teroristické nebo zapříčiněné přírodou) a lidi. U zranitelnosti se opět používá hodnocení kategorizací měřítka: žádná (0), nízká (1-3), přiměřená (4-7), vysoká (8-9), velmi vysoká (10). Dále se spočítá celkové ohrožení vynásobením dopadu (anglicky impact) a zranitelnosti (anglicky vulnerability). Změřené riziko se vyhodnotí na základě stanoveného měřítka rizika: nízké (1-33), střední (34-69), vysoké (70-100). Po tomto kroku začne identifikace a vybírání aktiv s nejvyšší mírou rizika. Pomocí brainstormingu[11] se může přijít na alternativní řešení a zvládání jednotlivých krizových služeb. (Marquis, 2012)

[11] Brainstorming je skupinová technika, která se zaměřuje na generování co nejvíce nápadů na dané téma. Je založena na výkonu skupiny. Lidé ve skupině totiž na základě podnětů ostatních vymyslí více, než by vymysleli jednotlivě.

Tab. 2.6: Návrh tabulky konkrétního řešení metodou CRAMM

Název služby: **Data o zaměstnancích** **Vlastník služby:**						
	Důvěrnost **Veřejná (0), omezená (1-5), důvěrná (6-9), zabezpečená (10)**		**Integrita** **Nízká (1-3), přiměřená (4-6), vysoká (7-9), velmi vysoká (10)**		**Dostupnost** **nízká (1-3), přiměřená (4-7), vysoká (8-9), velmi vysoká (10)**	
Dopad (1-10)	10 / zabezpečená		9 / vysoká		7 / přiměřená	
Hrozby – seznam všech možných hrozeb	Zveřejnění	Ztráta	Hacking	Vstupní chyby	Selhání dodávky elektřiny	V ýpadek serveru, na kterém jsou uložena data
Zranitelnost (1-10) **Žádná(0),nízká(1-3), přiměřená(4-7),vysoká(8-9),velmi vysoká (10)**	10	4	9	4	4	1
Ohrožení (dopad X hrozby)	100 (10X10)	40 (10X4)	81 (9X9)	36 (4X9)	28 (7X4)	7 (7 X1)
Měřítko rizika	vysoké	střední	vysoké	střední	nízké	ní zké
Možná protiopatření	zabezpečení heslem					

Měřítko rizika: nízké (1-33), střední (34-69), vysoké (70-100)

Zdroj: (Marquis, 2012)

2.6.3.8 Krok 8: kontrolní doporučení

Během tohoto procesu se kontroluje, zda by mohlo být identifikované riziko zmírněno nebo zcela eliminováno. Cílem doporučení je redukovat stupeň rizika na IT systém a jeho data

v akceptovatelné míře. Následující faktory by měly být zváženy při doporučeních a alternativních řešeních pro minimalizaci nebo eliminaci identifikovaných rizik:

- efektivita doporučených možností (systémová kompatibilita),

- legislativa a regulace,

- politika organizace,

- provozní vliv,

- bezpečnost a spolehlivost.

Tyto kontrolní doporučení jsou výsledkem procesu risk assessmentu a poskytují vstup pro proces přesunutí rizik. Během tohoto jsou doporučené procedury a technické kontroly ohodnocovány a implementovány. Musí zde být poznamenáno, že všechny možné doporučené kontroly mohou být implementovány pro redukci ztráty. Pro určení, která z nich je požadována a příslušná pro specifickou organizaci, je třeba určit náklady na implementaci kontrol, které by měly být také posouzeny. (SNEDAKER, 2007)

2.6.3.9 Krok 9: Výsledná dokumentace

Když už je risk assessment zcela zkompletován (zdroje pohrom a zranitelnost jsou identifikovány, riziko ohodnoceno a kontrolní doporučení jsou poskytnuty), výsledky by se měly dokumentovat do oficiálního reportu. Tento report je řídíc a pomáhá vedoucímu managementu rozhodovat například nad politikou, procedurami a rozpočtem. Oproti auditu nebo vyšetřovacích reportech, které se starají o špatně fungující záležitosti, reporty risk assessmentu by neměly prezentovat vyčnívající záležitosti, ale díky systematickému a analytickému přístupu k ohodnocení rizik by měly pomoci řídícímu managementu pochopit rizika a alokovat zdroje pro redukování a korekci potencionálních ztrát. Report risk assessmentu by měl popisovat hrozby a zranitelnost, měřit rizika a poskytovat doporučení pro řízení implementace. (STONEBURNER, 2002)

2.6.4 Strategie zmírnění rizika

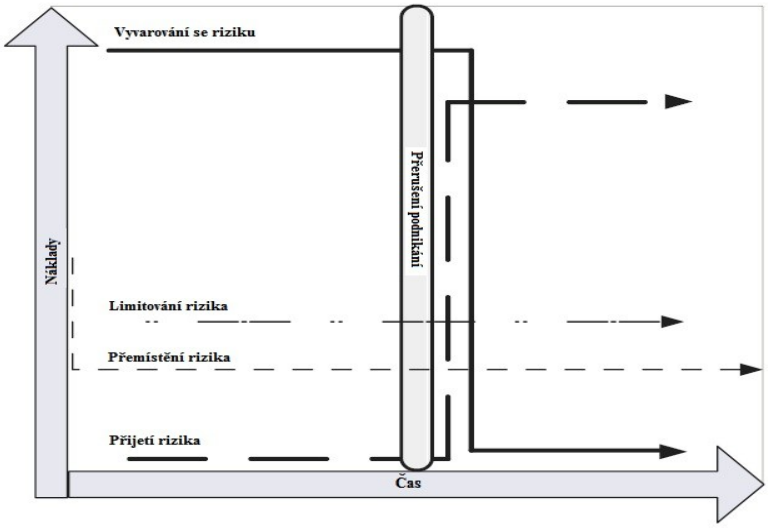
Zmírnění rizika je definováno jako podnikání takových kroků, které redukují nepříznivé efekty. Vývojem strategií zmírnění rizika je poslední fáze aktivit řízení rizik. Tato poslední část zahrnuje vstupy ohodnocení rizik a data z business impact analýzy. Je zde nutné se při vývoji strategie zmírnění rizika shodnout s profilem společnosti. Jestliže je ve firmě velká averze k riziku a tato firma vyžaduje vyhnutí se riziku za téměř každou cenu, strategie bude shodná s těmito cíli. Na druhou stranu, jestliže firmě nevadí vzít v potaz nějaké riziko,

strategie pak budou odlišné než v prvním zmíněném případě. Není zde pravidlo, že jedna strategie zmírnění rizika pasuje na každou firmu. Musí být proto vytvořena taková strategie, která bude souhlasit s firemními, finančními, operačními a cíli řízení rizik. (SNEDAKER, 2007)

2.6.4.1 Typy strategií zmírnění rizik, náklady a čas na obnovu

Zde bude zmíněno několik standardních strategií pro zmírnění rizik. Mezi tyto standardní volby se řadí tyto čtyři: přijetí, vyvarování se, limitování a přemístění rizika. Na následujícím obrázku jsou tato jednotlivá rizika zakreslena a jasně se nám ukazuje vztah mezi časem a náklady pro každou zvolenou variantu a relativní náklady pro každou možnost vzhledem k ostatním variantám.

Obr. 2.9: Náklady vs. čas při strategii zmírnění rizika



Zdroj: (SNEDAKER, 2007)

Přijetí rizika

Přijetí rizika nejde skutečně považovat za strategii zmírnění, protože riziko neredukuje svůj negativní efekt. I přesto je však akceptace rizika částí řízení rizik. Existuje několik důvodů, proč si společnosti mohou vybrat přijetí rizika v určité situaci. Nejběžnějším důvodem je to, že náklady na jiné možnosti řízení rizik, jako je například vyvarování se nebo limitování rizika, mohou převýšit náklady samotného rizika. Na druhou stranu, když už se vyvíjí strategie, měly by se vzít v úvahu důsledky při takzvaném "nic nedělaní“. Zde může být řešení, že se pojistíme tím, že se budou v případě potřeby provádět příslušné akce, protože

když se vezme v potaz důsledek akceptace rizika, jsou vidět potencionální následky a ty by se měly rozhodně zvážit vzhledem k dalším možnostem.

Na předešlém obrázku je vidět, že náklady na přijetí rizika jsou velmi nízké na začátku (rovnají se dokonce nule), ale po přerušení podnikání, či výpadku nějaké služby, mohou náklady stoupnout dokonce výše, než při jiných možnostech řízení strategie rizik. Možnost přijetí rizika je většinou používána u menších společností, které si často nemohou z finančních důvodů dovolit možnost jako je například vyhnutí se riziku. Přijetí rizika je nejméně nákladnou volbou v malém časovém období, ale na druhou stranu zase nejdražší variantou v dlouhém období. (SNEDAKER, 2007)

Vyvarování se riziku

Tato volba je opakem předchozí možnosti. V plánu obnovy je vyrovnání se riziku akce, která předchází absolutně působení rizika. Jestliže chceme předejít ztrátě dat, máme k dispozici zcela redundantní datové systémy nebo můžeme manuálně tyto systémy vypnout a přesunout zařízení s cennými daty předem na bezpečné místo a tímto se vyvarovat možné ztrátě způsobené blížícím se hurikánem. Tato varianta je nejdražší vzhledem k ostatním třem na začátku, ale náklady po výpadku služby jsou pak mnohem nižší. Takové vypnutí systémů, zabalení příslušného hardwaru a jeho přeprava do jiného místa je finančně náročné. Náklady na obnovu jsou ale zase minimální. Tato možnost není pro mnoho typů rizik a také pro hodně typů společností vůbec proveditelná. I přesto je tato možnost funkční a musí být zvážena při strategii zmírnění rizik. (SNEDAKER, 2007)

Limitování rizika

Jedná se o nejběžnější strategii při řízení rizik používanou v podnikání. Je zde vybráno limitování rizik skrze podnikání různých akcí. Například, když se provádí denní zálohy dat určitého systému ve firmě, jedná se o strategii limitování rizik. Toto řešení nezastaví diskovou jednotku od poruchy, neignoruje potencionální selhání disků, jen akceptuje, že diskové jednotky selhávají, a když už se to stane, máme zde náhradu, která nám pomůže se rychle dostat z této nepříznivé situace. Z předešlého obrázku je vidět, že limitování rizika je strategie, která náleží do skupiny mezi akceptaci rizika a vyhnutí se mu. Jde o jakousi střední cestu těchto dvou možností. Limitování rizika zahrnuje například: instalování firewallu, který udržuje sítě zabezpečené; vytváření záloh pro udržování dat v bezpečí; provádění cvičení proti požáru z bezpečnostních důvodů zaměstnanců a další. (SNEDAKER, 2007)

Tab. 2.7: Příklad možné strategie zálohování

Výběr kategorie	Možnost	Náklady, schopnost, service level agreements	Zmírnění rizika
Záloha dat – četnost	Neustálá	Drahá, nulová doba nečinnosti, překročí maximálně tolerovatelný výpadek (dále MTV).	Potencionální řešení závisí na nákladech pro implementaci.
	Denní	Rozumné náklady, do 8 hodin potencionální ztráty dat, 3 hodiny obnovy, splňuje MTV.	Implementace procesu denních záloh pro redukci pravděpodobnosti významné ztráty dat a redukci času obnovy pro splnění MTV.
	Týdenní	Rozumné náklady, do 5 dní potencionální ztráty dat, je potřeba 12 hodin k obnově, může splnit MTV.	
	Měsíční	Nízké náklady, nesplní MTV.	
Záloha dat – typ zálohy	Kompletní	Delší čas zálohy dat, kratší čas obnovy, shoduje se s MTV.	
	Postupný	Střední čas zálohy dat, delší čas pro obnovu, shoduje se s MTV.	
	Rozdílný	Střední čas zálohy, střední čas pro obnovu, shoduje se s MTV.	Tato možnost splňuje MTV s vynaložením nejnižších nákladů.
Záloha dat – metody zálohy	Záloha na pásku	Delší čas obnovy, nejméně nákladný, nemusí se vždy shodovat s MTV.	
	Elektronický trezor	Dlouhý čas obnovy, poněkud nákladné řešení, nemusí splnit MTV	
	Zrcadlení disků	Rychlý čas obnovy, střední náklady, může splnit MTV.	Založený na omezeních nákladů, tato volba se může shodovat s MTV.
	Vzdálené zrcadlení disků	Neustálá dostupnost, nulový čas na obnovu, nejdražší řešení, převyšuje MTV.	

Zdroj: (SNEDAKER, 2007)

Přemístění rizika

Způsob přemístění rizika znamená přesunutí rizika ochotné třetí straně. Hodně firem využívá outsourcingu určitých služeb, jako jsou zákaznické služby, uspokojení objednávek nebo mzdové služby. V praxi se to dělá v mnoha případech a díky tomu se firma může soustředit na své hlavní povinnosti související s podnikáním. Pokud si vybíráme například firmu, která poskytuje outsourcingem mzdové služby, můžeme si ji vybrat ze zcela jiného regionu a díky tomu se pojistit proti případným katastrofám, které jsou třeba tam, kde sídlí firma celkem běžné. Dalším příkladem přemístění rizika je sjednání pojištění nebo jiného typu pojišťovací služby. Na obrázku je opět vidět vztah této služby k ostatním možnostem přemístění rizika a bude obvykle stát více z důvodu neustálého placení poplatků za pojištění. V konečném důsledku však budou náklady zhruba na stejné úrovni jako u limitování rizika. Může se zdát, že se limitování rizika a jeho přemístění se jeví jako podobné varianty, ale je důležité pamatovat na trvání nákladů týkajících se těchto strategií. (SNEDAKER, 2007)

Náklady a čas na obnovu

Když už je vytvořen seznam požadavků na obnovu, měl by se pak zhodnotit také čas každé možnosti. Musíme zde stanovit maximálně tolerovatelný výpadek pro jednotlivé procesy, který je přijatelný. Možnost, která toto nesplňuje, by měla být odstraněna a nahrazena jinou, která splňuje zadaná kritéria. Další důležitou metrikou jsou také náklady vybrané varianty na obnovu. Ve většině případů platí, že pokud se jedná o vyšší schopnost zmírnění možného rizika, náklady na takovéto činnosti jsou pak vyšší. Jsou zde také další atributy, které by měly být zahrnuty při hodnocení nákladů. Jsou to tyto následující:

- náklady (náklady zvolené volby na zmírnění nebo obnovu),
- schopnost řešení,
- úsilí (množství úsilí, které bude vynaloženo na implementování a řízení zvolené volby),
- kvalita (kvalita produktu, služby nebo dat spojených s touto volbou),
- kontrola (množství kontrol společnosti, které budou zachovány během kritického business procesu),
- bezpečnost,
- zabezpečení (odhad fyzického a virtuálního zabezpečení, které možnost poskytuje). (SNEDAKER, 2007)

Pro lepší přehlednost jednotlivých atributů je vhodné zde vytvořit matici, která nám poskytne souhrnný přehled. V následující tabulce je srovnání varianty možnosti vztahující se k pořízení vlastního IT systémů. Další tabulka ukazuje možnost zřízení náhradního IT zařízení.

Tab. 2.8: Příklad možností pro pořízení kritického IT systému

Možnost	Náklady	Způsobilost	Úsilí	Kvalita	Možnost kontroly	Zabezpečení dat	Bezpečnost dat	Potřebnost
Když potřebujeme	Vysoké	Neznámá	Vysoké	Nízká	Nízká	Nízké	Nižší	Nízká
Předem zařízeno	Střední	Splní požadavky	Střední	Střední	Střední	Střední	Střední	Střední
Předem stanovený	Nízké	Splní požadavky	Nízké	Vysoká	Vysoká	Vysoké	Vysoká	Střední

Zdroj: (SNEDAKER, 2007)

Tab. 2.9: Příklad možností pro zřízení alternativního IT zařízení

Možnost	Náklady	Způsobilost	Úsilí	Kvalita	Možnost kontroly	Zabezpečení dat	Bezpečnost dat	Potřebnost
Firemní záložní sítě	Střední	Splňují požadavky	Střední	Nízká	Vysoká	Střední	Vysoké	Střední
Sítě provozovány outsourcingem	Vysoké	Splňují požadavky	Nízké	Vysoká	Nízká	Vysoké	Střední	Střední

Zdroj: (SNEDAKER, 2007)

Musí být pamatováno, že tyto možnosti mohou být zvažovány jen proto, že splňují časové požadavky obnovy.

Důležité je také již dříve zmiňovaná dohoda service level agreements (dále SLA) v případě obnovy služby, kterou firma provozuje outsourcingem. Tyto metriky spadají všechny pod kategorii service level agreements a mohou zahrnovat množství různých elementů, jako jsou například:

- doba odezvy v případě počátečního požadavku služby,

- technická kapacita (specifikace počítačového vybavení, místo na paměti, hlasové a datové kapacity, rychlost, rozsah dostupnosti a další),
- přístup k zařízení a vybavení pro obnovu,
- přístup k adekvátní pracovní oblasti a přístup zaměstnancům,
- bezpečnostní procedury a garance,
- kontroly procesů,
- přístup k technické a funkční podpoře (čas, doba odezvy apod.). (SNEDAKER, 2007)

Je zde doporučeno, aby smlouvy service level agreements byly kontrolovány a zahrnuty do business impact analýzy jako kritické podniková funkce.

Shrnutí strategie zmírnění rizik

Tyto kroky jsou doporučovány při vývoji strategie zmírnění rizik:

- sesbírat data pro obnovu,
- porovnat náklady, způsobilost a možnosti úrovně služeb v každé kategorii,
- specifikovat způsoby vyrovnání se s rizikem (akceptace rizika, vyhnutí se riziku, limitování nebo přesun rizika) a které z nich jsou nejvíce potřebné,
- vybrat možnost, která nejlépe splní firemní potřeby. (SNEDAKER, 2007)

2.6.5 Vývoj plánu, testování a audit

V této konečné fázi by již měl být plán realizován. Musíme dát dohromady data, která byla předtím zjištěna a seřadit je do přehledné podoby plánu obnovy. Plán by měl být také testován bez ohledu na to, zda bude někdy implementován. Díky tomu bude jasně definováno, jak a kdy bude aktivován plán obnovy. Pokud plán projde testováním je pak dobré, ještě provést audit celkového plánu obnovy.

2.6.6 Udržování plánu

Ve firmách není nic definitivního. Všechno se určitým způsobem vyvíjí a mění. Z tohoto důvodu by měl i plán obnovy být neustále přepracováván a obnovován v případě jakýkoliv změn, které se týkají fungování procesů ve firmě. V následující části budou probrány typy změn, které se objevují v podnikání a vliv těchto změn na plán obnovy. Tyto změny se dělí do následujících pěti kategorií:

- technologické změny (updaty nebo změny v softwaru, hardwaru a dalších technologií),
- změny v podnikání (změny v procesech nebo při přemístění podniku),

- změny v personálu (změny v organizačním uspořádání či odděleních a individuální zodpovědnosti),
- obchodní změny (změna způsobu vytváření ceny produktů nebo služeb a změny našich zákazníků, jak spotřebovávají a co si myslí o těchto produktech nebo službách),
- externí změny (další události, které se objevují v prostředí podniku a určitým způsobem mohou změnit rizika našeho podnikání). (GREGORY, 2008)

3. Analýza současného stavu

3.1 Firma a procesní řízení

Diplomová práce je zpracovávána v reálné firmě, která se zaměřuje na poskytování služeb. Firma je procesně řízena. Tím se rozumí soubor činností týkajících se plánování a sledování výkonnosti především realizačních firemních procesů. Procesní řízení je založeno na využití znalostí, zkušeností, dovedností, nástrojů, technik, systémů k definování, vizualizaci, měření, kontrole, informování a zlepšování procesů s cílem splnit požadavky zákazníka za současné optimální rentability aktiv. (Procesní, 2007)

Firma se díky tomuto soustředí na filozofii řízení procesu od počátku do konce. Aplikace tohoto řízení je prováděna systematickým a datově orientovaným přístupem, který směřuje ke zlepšování výkonnosti organizace. Identifikuje nám možné příležitosti ke zlepšení za použití ověřených metod řešení problémů. Pomůže nám také s vyhodnocením v případě potřeby změny funkcí systému s cílem zajistit to nejefektivnější a nejhospodárnější provádění procesu. Při vyhodnocení můžeme také identifikovat příležitosti ke zlepšení kvality, provozní výkonnosti a trvalého uspokojování našich zákazníků. Procesní řízení tedy označuje soubor činnosti, které firma provádí buď za účelem optimalizace klíčových procesů, nebo je přizpůsobuje v případě nových potřeb. (Procesní, 2007)

Ve firmě, pro kterou je diplomová práce zpracovávána, jsou procesy formalizovány. Je zde zaveden ITIL pro řešení vybraných oblastí managementu IT služeb.

3.2 Současný stav plánu obnovy ve společnosti

Disaster recovery proce (dále jen DRP), tedy plán obnovy, je ve firmě vypracován pro její kritické činnosti. DRP pro nekritické činnosti není zcela přesně specifikován, a proto se zde vytváří potřeba tento plán vypracovat do ucelené a komplexní podoby, aby byla v případě nutnosti zabezpečena kontinuita těchto nekritických služeb a vědělo se přesně, jak v takovýchto situacích postupovat. Práce na plánu obnovy nekritických informačních služeb již začaly. Business impact analýza již byla provedena.

3.3 Cíl plánu obnovy nekritických služeb

Prvotním úkolem pro diplomovou práci je popis probíhajících nekritických procesů ve firmě a vytvoření konkrétního postupu pro analýzu rizik, které mohou tyto činnosti narušit. Tímto bude směřováno k analýze rizik a výslednému zpracování zjištěných výsledků. V plánu

obnovy by měly být i zmíněny jednotlivé návrhy a opatření při výpadku analyzovaných služeb. Bude se tedy postupovat:

- popsáním fungování nekritických služeb ve firmě,
- ohodnocením výpadků služeb,
- návrhem možných protiopatření při výpadku,
- konečným zpracováním výsledků.

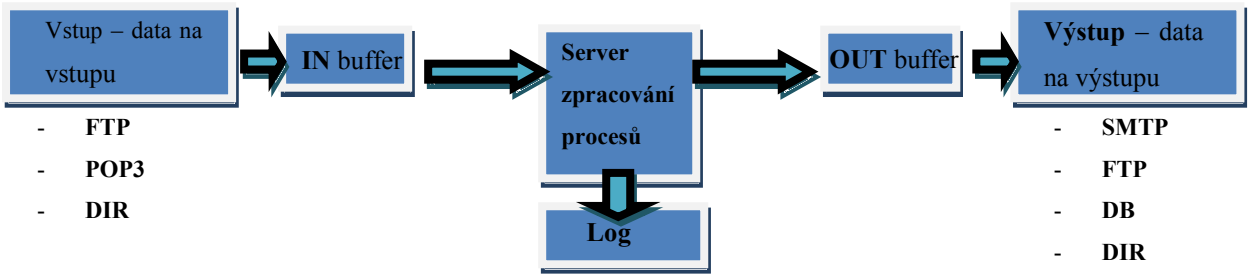
4. Návrh procesu obnovy

V návrhu bude popsáno, jak se postupovalo, při návrhu procesu obnovy nekritických informačních služeb v reálné firmě. Je vycházeno ze skutečnosti, že práce na plánu pro obnovu nekritických služeb již začaly. Proces analýzy služeb, business impact analysis, je již zpracován. Díky tomu se určilo, které služby jsou nekritické. Tato práce je zaměřena konkrétně na návrh obnovy pro hlavní podpůrný ekonomický systém firmy. Jde o enterprise resource planning, tedy ERP[12].

4.1 Analýza faktorů ohrožení funkcionality ERP

Nekritické procesy ve firmě jsou realizovány za použití několika IT služeb (sofwarových produktů), které slouží pro řízení podniku a podporují následující procesy, jako jsou například: finanční účetnictví, evidence majetku, řízení lidských zdrojů nebo podpora prodeje a dalších. Samotný ekonomický systém se skládá z dalších modulů a právě analýza fungování tohoto systému nám objasní případy, kdy se mohou vyskytnout konkrétní výpadky při jeho provozu. Na následujícím obrázku je vyobrazeno schéma toku dat tohoto podpůrného ekonomického systému.

Obr. 4.1: Schéma toku dat podpůrným ekonomickým systémem



Zdroj: interní materiály společnosti

Nejprve jdou data z podpůrného ekonomického systému (dále jen ERP) na vstup. Tyto data mohou být různého druhu. Tento vstup slouží pro přenos těchto dat. Mohou být uložena na FTP serveru. Zkratka FTP znamená v informatice protokol, který se používá k přenosu souborů mezi počítači za pomoci počítačové sítě. FTP využívá pro své fungování protokol TCP z rodiny TCP/IP[13]. Dalším typem serveru je POP3[14] a slouží pro stahování emailových

[12] ERP je zkratka od slov enterprise resource planning. Jedná se o informační systém, který integruje a automatizuje velké množství procesů, které souvisí s produkčními činnostmi podniku. Jde o výrobu, logistiku, distribuci, správu majetku, prodej, fakturaci a účetnictví.

[13] TCP/IP obsahuje sadu protokolů pro komunikaci v počítačové síti a jedná se o hlavní protokol celosvětové sítě internet. Lze být využíván nezávisle na použitém operačním systému, je tedy nezávislý na dané platformě Tento komunikační protokol je množina pravidel, které určují syntaxi a význam jednotlivých zpráv při komunikaci. TCP protokol je spolehlivý, tedy doručí adresátovi data v pořádku a ve správném pořadí.

zpráv ze vzdáleného serveru na klienta. Jiný typ je zase server databáze[15], kde je uložena množina informací. A konečně úložný prostor typu DIR, který je lokální a slouží firmě pro ukládání interních dat. Další komponentou při zpracovávání dat je buffer IN. Zde se ukládají data ze vstupu, která se pak dále předávají ke zpracování. Data na IN bufferu se ukládají až do provedení zálohy, která se provádí v pravidelných intervalech. Zároveň při selhání zpracování dat v následujícím kroku, je možno tyto data zpětně vyhledat a znovu obnovit či opakovaně zpracovat požadovanými procesy. Dále z IN bufferu putují data do serveru pro zpracování procesů. Jedná se o server, kde probíhají veškerá zpracování dat. Procesy zde mohou být naprogramovány dle požadavků firmy a charakteru zpracovávaných dat. Naprogramované procesy mohou také zahrnovat i kontrolní mechanizmy jako jsou například kontroly vstupních dat na jejich správný formát, který je zapotřebí pro úspěšné uložení do ERP. Současně je zde možnost zvolení ukládání jednotlivých procesů do takzvaného logu. Log je název pro záznam nebo soubor záznamů, které si zde server pro zpracování procesů vytváří pro ukládání informací o své činnosti a běhu. Logy pak slouží při zpětné analýze k rozpoznání, zda došlo k nějaké chybě a pokud ano, pak napomáhají určit a definovat k jaké chybě vlastně došlo a z jakého důvodu. Je zde také možnost logování vypnout. V případě chyby je však jednoduší nechat log zapnutý a díky jeho výpisům pak dohledat snadněji chybnou transakci. Následující komponentou při dalším kroku je buffer OUT. V tomto bufferu se přechodně ukládají data, která byla zpracována. Opět se zde v jistých časových intervalech tato data zálohují a jsou pak k dispozici v případě potřeby při náhodném a nečekaném výpadku. Předposlední komponentou je výstup. Zde se ukládají již zpracovaná data, která se dále nahrávají do ERP. Opět jsou zde servery například SMTP[16], který slouží pro přenos zpráv elektronické pošty. Dalšími typy serverů jsou již zmiňované FTP, DB a DIR.

Podpůrný ekonomický systém funguje na několika serverech. Jeden server je na vývoj, druhý na potřeby testování a třetí ten nejdůležitější je server produkce, tedy část, kde probíhají všechny důležité činnosti potřebné pro zpracovávání procesů firmy. Na vývojovém serveru se procesy vyvíjejí a dále odlaďují. Na testovacím se již zpracovávané procesy testují, zdali vše správně funguje a zdali mohou být nasazeny do reálného provozu. Poslední části je server produkční. Je složen z dvou diskových polí (aplikačních serverů). Je to z toho důvodu, že

[14] POP3 je internetový protokol pro stahování emailových zpráv. Jde o aplikační protokol pracující přes TCP/IP připojení.

[15] Databáze - v širším smyslu jsou součástí databáze také softwarové prostředky, které umožňují manipulaci s uloženými daty a konečný přístup k nim. Tento software se nazývá systém řízení báze dat (SŘBD).

[16] SMTP - Simple Mail Transfer Protocol, je internetovým protokolem elektronické pošty. Protokol nám zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. Zpráva je zde doručena do takzvané poštovní schránky adresáta, ke které pak může kdykoli třeba i offline přistupovat

produkční server používá mnoho uživatelů a kvůli tomu je pak třeba rozdělit zátěž na dva disky. FTP server neobsahuje, ten je však připojen k tomuto produkčnímu serveru zvlášť.

4.1.1 Oblasti výpadků systému

Nekritické informační služby běží na podpůrném ERP ekonomickém systému. Z hlediska rizika služeb zde mohou nastat výpadky:

- infrastruktury,
- aplikační chyby.

4.1.1.1 Výpadky infrastruktury

Infrastrukturou se rozumí výpadek softwaru a hardwaru. Pokud se objeví chyba takovéhoto charakteru, je zde nutné přímo volat zodpovědnému pracovníkovi firmy, která poskytuje outsourcing služby. Může se jednat třeba jen o výpadek síťového prvku (například routeru). Výpadek je potom možno opravit v kritických případech i v rámci 4 hodin. Takovéto výpadky se ovšem nedají odhadnout. V horším případě může selhat přímo hardware, tedy diskové pole, na kterém jsou uložena data, se kterými potřebujeme pracovat. Chyby tohoto charakteru jsou řešeny společností poskytující outsourcing, jiná možnost není.

4.1.1.2 Aplikační chyby

Aplikační chyby jsou již selháním na straně uživatele. Většinou je možnost si tyto chyby opravit vlastnoručně nebo alespoň kontaktováním vlastníka procesu přímo ve firmě. Mohou se objevit tyto chyby:

- špatná data na vstupu nebo výstupu,
- chybná struktura,
- patchovaní.

V těchto případech je pak nutno kontaktovat vlastníka procesu anebo jinou zodpovědnou osobu ve firmě.

Shrnutí hlavních oblastí ohrožení výpadků ERP infrastruktury a aplikačních chyb:

- nefunkční produkční systém,
- nefunkční vývojový systém,
- nefunkční testovací systém,
- nefunkční FTP server 1/server 2,
- nefunkční server pro zpracování procesů,
- nefunkčností infrastruktura (datové sítě),

- nefunkčnost koncového zařízení (PC).

4.1.2 Ohodnocení potencionálních ohrožení ERP

Bude tady řešeno ohodnocení potencionálního ohrožení ERP systému. V předešlé kapitole byly určeny oblasti výpadku systému. Jsou rozděleny na oblast výpadků infrastruktury a aplikačních chyb. V následujících dvou tabulkách jsou uvedeny všechny možné hrozby, které se mohou vyskytnout právě v oblasti infrastruktury a aplikačních chyb. Bylo třeba vytvořit konkrétní stupnici pro ohodnocení pravděpodobnosti a dopadu. Při tvorbě uvedené stupnice bylo vycházeno z metodiky CRAMM, která byla popsána v části praktické. Pravděpodobnost zde byla stanovena stupnicí:

- 1: nízká znamená, že zdroj hrozby nemá dostatek motivace, schopnosti anebo kontroly jsou natolik preventivní, že je velmi nízká pravděpodobnost výpadku služby,
- 3: střední zdroj hrozby je motivovaný, ale kontroly mohou pomoci zabránit výpadku,
- 5: vysoký, je vysoká pravděpodobnost vzniku hrozby, zdroj je vysoce motivovaný a preventivní kontroly jsou většinou neefektivní a neúplné.

U dopadu je opět stanovena konkrétní stupnicí:

- 1: žádná znamená, že dopad není žádný nebo jen nepatrný,
- 2: nízká značí, že dopad je nízký, ale nevede ke ztrátám majetku,
- 3: přiměřená popisuje, že dopad kromě menší ztráty majetku vede k ovlivnění pověsti organizace,
- 4: vysoká definuje, vysokou ztrátu na majetku a ovlivnění celkové pověsti organizace,
- 5: velmi vysoká může vést k velmi nákladné ztrátě na hmotném majetku, která může výrazně porušit fungování firemních procesů a brání organizaci v jejím poslání, v krajním případě může mít za následek i zranění osob.

Samotný výpočet ohrožení vznikne vynásobením ohodnocení pravděpodobnosti a dopadu. Účelem tohoto výpočtu je posouzení stupně rizika konkrétní hrozby pro firmu. Změřené riziko se vyhodnotí na základě stanoveného měřítka rizika, jako: nízké (1-8), střední (9-17) a vysoké (18-25).

Tab. 4.1: Ohodnocení chyb v infrastruktuře

Hrozby - seznam možných hrozeb	Pravděpodobnost 1, 3 a 5	Dopad 1-5	Výpočet ohrožení = pravděpodobnost x dopad
Nefunkční produkční systém – systém nelze konektovat	1	5	5
Nefunkční testovací systém – systém nelze konektovat	1	3	3
Nefunkční vývojový systém – systém nelze konektovat	1	5	5
Nefunkční FTP server 1 pro produkční systém – systém nelze konektovat	1	5	5
Nefunkční FTP server 2 pro systém testování a vývoj – systém nelze konektovat	1	5	5
Nefunkční FTP server 1 pro produkční systém – vypršela platnost uživatelského účtu	2	5	10
Nefunkční FTP server 2 pro systém testování a vývoj – vypršela platnost uživatelského účtu	1	5	5
Nefunkční Server pro zpracování procesů – server 3 mimo provoz	1	5	5
Nefunkčnost podpůrné infrastruktury (především síťové prostředí)	3	4	12
Nefunkčnost koncového zařízení (PC)	3	2	6

Zdroj: interní informace firmy

Celková analýza nám vyšla dobře a to z toho důvodu, že při výpočtu nevznikl žádný výskyt vysokého ohrožení. Dvě hrozby se však řadí do rizika středního. Jde o nefunkční FTP server pro produkční systém, díky vypršení platnosti uživatelského účtu a nefunkčnost podpůrné infrastruktury (především síťového prostředí). Nesmí se ale opomenout ani rizika, která se zařadila do kategorie nízká. Tady se také musí navrhnout příslušná opatření v případě výskytu hrozby. V další tabulce jsou ohodnoceny aplikační chyby. Stupnice ohodnocení pravděpodobností, dopadů a výpočtu ohrožení je stejná, jako v tabulce předchozí.

Tab. 4.2: Ohodnocení aplikačních chyb

Hrozby - seznam možných hrozeb	Pravděpodobnost 1, 3 a 5	Dopad 1-5	Výpočet ohrožení = pravděpodobnost x dopad
Nefunkční Server pro zpracování procesů – nefunkční server (chyba infrastruktury) nebo nefunkční aplikace v Serveru pro zpracování procesů – nefunkční server 3 jako celek	1	5	5
Nefunkční Server pro zpracování procesů – server 3 funkční, jen se objevil „zamrzlý proces“	3	2	6
Nefunkční proces na Serveru zpracování procesů – chybí data ze zdrojového systému (z IN bufferu)	3	2	6
Nefunkční proces na Serveru zpracování procesů – chybí data na cílovém systému (z OUT bufferu)	3	2	6
Nefunkční proces ERP – chyba při zpracování vstupních dat	3	2	6
Nefunkční proces ERP – chyba při zpracování výstupních dat	3	2	6
ERP modul nefunkční v důsledku implementace patche	3	4	12

Zdroj: interní informace firmy

Pří ohodnocení aplikačních chyb nám vyšlo jen u jedné hrozby střední měřítko rizika a to u nefunkčního ERP modulu v důsledku implementace patche.

Tyto dvě tabulky byly zpracovány na základě poznatků odpovědných pracovníků firmy. Konkrétní ohodnocení pravděpodobnosti a dopadu bylo stanoveno díky subjektivnímu hodnocení zodpovědných expertů. Na základě vypracované analýzy byl vyřešen návrh postupu pro řešení výpadků v souladu s procesy ve firmě.

4.2 Návrh postupu pro řešení výpadků ERP

Z vypracované analýzy rizik z předešlé kapitoly byl vypracován návrh postupu řešení výpadků ERP systému firmy. Výpadek tedy může nastat buď u infrastruktury, nebo se jedná o aplikační chybu. Chyby v infrastruktuře nelze nijak přímo ve firmě zprovoznit. Většinou se jedná se incident, přímo na straně společnosti, která nám službu poskytuje outsourcingem. V tomto případě je třeba kontaktovat příslušnou zodpovědnou osobu a problém co nejrychleji vyřešit. V případě aplikačních chyb již lze chyby koordinovat, řídit a opravovat v rámci firmy. Jedná se o chyby typu špatných dat na vstupu nebo na výstupu či chybějících údajů, které jsou ERP systémem striktně vyžadovány. U takovýchto aplikačních chyb je důležitý vlastník procesu a ten by měl být kontaktován v případě takovéhoto selhání.

V následujících dvou tabulkách, je vypracován návrh postupu pro řešení potencionálních výpadků, které mohou v průběhu operací nekritických služeb nad ERP systémem vzniknout. V každé tabulce je popsán popis výpadku. V dalších sloupcích je stanoven návrh doby pro obnovu, první kontaktní osoba a také možná opatření. V první tabulce jsou popsány výpadky v infrastruktuře, ve druhé zase aplikační chyby.

Tab. 4.3: Analýza potencionálních výpadků v infrastruktuře a návrh jejich řešení

Výpadky infrastruktury – nedostupnost báze dat, fyzický výpadek nebo služba nefunguje			
Popis výpadku	**Stanovená doba obnovy (ve SLA)**	**První kontakt**	**Možná opatření**
Nefunkční produkční systém – systém nelze konektovat	Do 4 hodin	Pracovník podpory báze a infrastruktury ekonomického systému	Kontrola funkce FTP serveru, kontakt pracovníka podpory báze. Vyžadovat odpovídající podporu v rámci SLA. Zanesení požadavků do SLA a dodržování procesů v souladu se Service Level Management.
Nefunkční testovací systém – systém nelze konektovat	Do 1 dne	Pracovník podpory báze	Kontaktovat bázistu serveru
Nefunkční vývojový systém – systém nelze konektovat	Do 3 dnů	Pracovník podpory báze	
Nefunkční FTP server 1 pro produkční systém – systém nelze	Do 4	Pracovník	

konektovat	hodin	podpory báze	
Nefunkční FTP server 2 pro systém testování a vývoj – systém nelze konektovat	Do 1 dne	Pracovník podpory báze	
Nefunkční FTP server 1 pro produkční systém – vypršela platnost uživatelského účtu	Do 4 hodin	Pracovník podpory báze	Kontaktovat bázistu serveru – neměl by dle SLA vůbec nastat, jedná se o problém bezpečnosti.
Nefunkční FTP server 2 pro systém testování a vývoj – vypršela platnost uživatelského účtu	Do 1 dne	Pracovník podpory báze	
Nefunkční Server pro zpracování procesů – server 3 mimo provoz	Do 4 hodin	Pracovník podpory báze	Kontaktovat bázistu serveru
Nefunkčnost podpůrné infrastruktury (především síťové prostředí)	Do 4 hodin	Help desk/podpora síťové infrastruktury	Dle SLA
Nefunkčnost koncového zařízení (PC)	Do 3 dne	Help desk/lokální správce	Dle SLA

Zdroj: interní informace firmy

Tab. 4.4: Analýza potencionálních aplikačních chyb a návrh jejich řešení

Aplikační chyby – výpadky aplikačního serveru		
Popis chyb	**První kontakt**	**Možná opatření / příčina chyby**
Nefunkční Server pro zpracování procesů – nefunkční server (chyba infrastruktury) nebo nefunkční aplikace v Serveru pro zpracování procesů – nefunkční server 3 jako celek	Pracovník podpory serveru pro zpracování procesů	Diagnostika HW a jeho oprava.
Nefunkční Server pro zpracování procesů – server 3 funkční, jen se objevil„zamrzlý proces“	Pracovníci 1, Pracovník 2 a pracovník 3	Zastaví se Server pro zpracování dat přes speciálního klienta, kontrolují se jednotlivé probíhající procesy
Nefunkční proces na Serveru zpracování procesů – chybí data ze zdrojového systému (z IN bufferu)	Business incident team	Kontrola vstupního připojení, kontaktování podpory pro vstupní data
Nefunkční proces na Serveru zpracování procesů – chybí data na cílovém systému (z OUT bufferu)	Business incident	Kontrola výstupního připojení, zopakování přenosu, kontaktování

	team	podpory pro výstupní data
Nefunkční proces ERP – chyba při zpracování vstupních dat	Business incident team	Zkontrolovat vstupní data na FTP serveru, kontaktování konzultanta nebo super uživatele modulu ERP / neúplná data, mimo číselníková data
Nefunkční proces ERP – chyba při zpracování výstupních dat	Business incident team	Zkontrolovat výstupní data, případně kontaktovat konzultanta nebo super uživatele modulu ERP / neúplná data, mimo číselníková data
ERP modul nefunkční v důsledku implementace patche	Business incident team	Kontaktování konzultanta a uvědomění uživatelů dotčených poruchou

Zdroj: interní informace firmy

Tabulky návrhů pro obnovu výpadků infrastruktury a aplikačních chyb byly navrhnuty ve spolupráci se zodpovědnými pracovníky firmy.

4.2.1 Shrnutí možných výpadků

Výpadky mohou vzniknout v důsledku výpadku infrastruktury nebo kvůli aplikačním chybám. V případě výpadku infrastruktury se postupuje dle podmínek, které jsou stanoveny ve smlouvě SLA. Jedná se o případy:

- selhání hardwaru (příkladem je výpadek síťového prvku nebo selhání celého diskového pole),
- selhání softwaru (jde o vypršení planosti hesla systémových účtů na FTP nebo jiných souborových systémech).

Pokud vzniknou aplikační chyby, je možnost si je opravit přímo ve firmě, tedy není zde nutnost kontaktovat firmu, která nám službu poskytuje outsourcingem. Aplikační chyby tedy mohou vzniknout:

- zadáním špatného formátu dat na vstupu nebo na výstupu (ERP požaduje u faktury číselné označení dokladu, to je však navedeno v jiném formátu, než systém podporuje a z toho důvodu se už se jedná o špatná data),
- chybná struktura (u formuláře jsou nutné čtyři identifikační údaje, ale u jednoho formuláře jsou zadány jen údaje tři – díky kontrolním procesům se na chybu v serveru pro zpracování procesů může přijít a lze tuto chybu i opravit),

- zadání nepodporovaného obsahu,
- chyby z důvodu implementování patche (v testovacím systému procesy fungovaly, ale po implementaci patche do „ostrého“ produkčního systému nemusí některé procesy, které před tím fungovaly, běžet).

5. Zhodnocení navrhovaného řešení

Analyzované nekritické služby běží na podpůrném ekonomickém ERP systému. Jeho fungování zde bylo podrobně popsáno a rozděleno na výpadky v infrastruktuře a chyby aplikační. Při návrhu bylo vycházeno z rámce ITIL. Při ohodnocení potencionálních výpadků ERP systému se postupovalo, dle metodologie CRAMM. Na základě této analýzy byl vypracován důkladný komunikační plán a byly navrhnuty opatření pro obnovu nekritických informačních služeb. Zpracované řešení bude použito v reálné firmě, kde se zformuluje do konkrétního DRP pro obnovu nekritických služeb. Doporučená protiopatření se zde budou týkat hlavně firmy, která poskytuje služby formou outsourcingu. Musí se přesně specifikovat požadavky do smlouvy. Jedná se o smlouvu service level agreements, ve zkratce již zmiňované SLA. Toto se bude týkat výpadků v infrastruktuře. Oproti tomu pro chyby aplikační je zpracován komunikační plán, a jsou určeny osoby, které jsou zodpovědné za jednotlivý proces firmy.

Navrhované řešení popsané v praktické části, je proveditelné a vzniklo na základě zkušeností a expertního ohodnocení pověřenými odpovědnými pracovníky firmy. Cíl práce, návrh procesu obnovy nekritických informačních služeb, byl splněn.

6. Závěr

V úvodní kapitole bylo popsáno, proč jsou IT služby ve firmách tak důležité a proč bychom se o ně měli vůbec zajímat. Právě jejich výpadek může způsobit menší, ale i velké problémy. Proto by se tyto možné výpadky neměly brát na lehkou váhu, ale musíme jim být schopni čelit. A to můžeme jen tehdy, budeme-li připraveni a máme-li precizně zpracován plán pro obnovu všech možných hrozeb.

Ve druhé části jsou popisována teoretická východiska práce a pojmy problémové oblasti. Popisuje se historie rámce ITIL a důvod jeho vzniku. ITIL se dále definuje a jsou srovnány jeho jednotlivé verze a rozdíly mezi nimi. Dále se klade důraz na důležité složky podnikání při návrhu postupu obnovy. Jedná se o souhru lidí, procesů a technologií. Je přiblížen také demingův kruh kvality, který by neměl být opomenut při jakémkoli rozhodování. V neposlední řadě je zde zmíněna smlouva SLA, tedy service level agreement. Ta definuje přesná pravidla pro firmu, která poskytuje služby outsourcingem. V kapitole zabývající se procesem plánování a jednotlivými kroky při plánování procesů obnovy, jsou vypsány tyto jednotlivé doporučené etapy při navrhování plánu obnovy. Jedná se o kroky: inicializace projektu, ohodnocení rizik, business impact analysis, strategie zmírnění rizika, vývoj plánu, testování, audit a udržování plánu.

Ve třetí kapitole je popisována analýza současné stavu ve firmě. Diplomová práce je vypracována pro reálnou společnost, která se zaměřuje na poskytování služeb. Firma má procesy formalizovány a je zde zaveden ITIL pro řešení vybraných oblastí managementu IT služeb. Současný stav plánu obnovy ve společnosti existuje jen pro kritické činnosti. Nekritické služby tento plán nemají zcela přesně vypracován. Vytváří se požadavek na plán obnovy. Jsou shrnuty cíle, kterých chceme dosáhnout.

Čtvrtá kapitola se týká konkrétního návrhu obnovy nekritických služeb v reálné společnosti. Práce na plánu obnovy začaly, tedy business impact analýza již byla provedena. Zaměřujeme se konkrétně na návrh obnovy pro hlavní podpůrný ekonomický ERP systém firmy, na kterém analyzované nekritické služby fungují. Začíná se popisem procesů systému a analýzou faktorů ohrožení funkcionality. Z toho vychází jednotlivé možné oblasti výpadků systému. Dělí se na výpadky infrastruktury a chyby aplikační. Tyto výpadky se ohodnocují. Je zde stanovena stupnice hodnocení pravděpodobnosti a dopadu. Je vycházeno z metodologie CRAMM. U hrozeb je vypočteno ohrožení, které vznikne vynásobením pravděpodobnosti s dopadem. Výsledkem tohoto ohodnocení je fakt, že jen určité měřítko hrozeb je definováno jako střední. Ostatní jsou označeny za nízké a vysoký podíl je nulový. Díky tomu se určí

návrh postupu pro řešení výpadků ERP. U infrastruktury nám vyšlo, že je podstatné stanovit odpovídající podmínky dle SLA smlouvy. Zanesení přesných požadavků do SLA nám zajistí plynulé fungování služeb. Pokud se přeci jen nějaký ten výpadek objeví, je v této smlouvě stanovena maximální doba obnovy, do které musí outsourcingová společnost chybu opravit. Bylo také stanoveno, jaký pracovník je za konkrétní výpadek odpovědný, zde je to pracovník podpory báze a infrastruktury ekonomického systému. V případě nefunkčnosti podpůrné infrastruktury firmy nebo nefunkčnosti koncového zařízení (PC), je třeba opět kontaktovat firmu, která je za vedení této služby zodpovědná. Možné řešení a požadovaný časový interval se musí stanovit přesně ve SLA. V případě výpadku se přímo kontaktuje helpdesk, který slouží pro podporu síťové infrastruktury, kde nám pomohou problém vyřešit. Pokud nastanou chyby aplikační, je uveden první kontakt na odpovědného pracovníka nebo vlastníka procesu. Jsou uvedeny i možná protiopatření, co se v případě uvedené chyby musí udělat. V jistých případech musí být kontaktován business incident tým, který se zabývá chybami a zpracovává návrhy řešení dle konkrétní povahy výpadku. Možná opatření jsou také stanovena u incident týmu. Návrhy pro obnovu výpadků byly vytvořeny ve spolupráci se zodpovědnými pracovníky firmy. V páté kapitole se zhodnotilo navrhované řešení.

Závěrem lze konstatovat, že cíle, které byly stanoveny v úvodu této práce, jsou splněny a navrhované řešení poskytne odpovídající základ pro vytvoření konkrétního návrhu procesu obnovy nekritických služeb ve firmě.

Seznam použité literatury

(BPM, 2003-2007) BPM slovníček: Výklad pojmů a zkratek z oblasti BPM a procesního řízení. *BPM portál*: *Znalostní servis profesionálů BPM. ISSN 1802-5676* [online]. Copyright © 2003-2007 [cit. 2012-02-12]. Dostupné z: http://bpm-slovnik.blogspot.com/2007/09/proces.html.

(Commerce, 2005) *Introduction to ITIL : Office of Government Commerce*. London : Office of Government Commerce, 2005. 242 s. ISBN 9780113309733.

(CRAMM, 2012) CRAMM: Information Security Toolset. *Risk analysis consultants* [online]. © 2012 [cit. 2012-02-20]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/CRAMM.

(GREGORY, 2008) GREGORY, P. *IT Disaster Recovery Planning For Dummies*. Hoboken: Wiley Publishing, Inc., 2008. 360 s. ISBN 978-0-470-03973-1.

(HOSPES, 2005) HOSPES, Jan. ITIL - Nejrozšířenější přístup k řízení informatiky. *IT Systems* [online]. 2005, 12/2005, [cit. 2011-10-19]. Dostupný z WWW: <http://www.systemonline.cz/clanky/itil-nejrozsirenejsi-pristup-k-rizeni-informatiky.htm>.

(Itil, 2007) *Itil* [online]. 2007 [cit. 2011-10-20]. Historie, vývoj a přínosy ITIL®. Dostupné z WWW: <http://www.itil.cz/index.php?id=983>.

(KIRVAN, 2011) KIRVAN, Paul. Business impact analysis questionnaire template. TECHTARGET. *SearchDisasterRecovery* [online]. [červen 2011] [cit. 2012-02-15]. Dostupné z: http://searchdisasterrecovery.techtarget.com/tutorial/Business-impact-analysis-questionnaire-template.

(Marquis, 2012)10 Steps to Do It Yourself CRAMM. MARQUIS, Hank. ITSM solutions: IT Experience. Practical solutions [online]. © 2012 [cit. 2012-02-09]. Dostupné z: http://www.itsmsolutions.com/newsletters/DITYvol4iss50.htm.

(Procesní, 2007) Procesní řízení. ITSM [online]. © 2007 [cit. 2012-04-04]. Dostupné z: http://www.itil.cz/index.php?id=914.

(Service, 2012) SLA smlouva. *Total service*: *Outsourcing Information Technology* [online]. 2012 [cit. 2012-04-03]. Dostupné z: http://www.totalservice.cz/cesky/sluzby-a-reseni/ICT-Outsourcing/service-level.html.

(SKÁLA, 2007) SKÁLA, Jiří . *ITIL : Best Practice řízení ICT služeb a ICT infrastruktury*. Praha, 2007. [cit. 2011-10-19] 10 s. Seminář. VŠE. Dostupné z WWW: <http://nb.vse.cz/~ridelj/vsomis/MIS_LS03_ITIL_clanek.pdf>.

(SLA, 2011) SLA (Service Level Agreement). *Uexcor systems* [online]. 18. 5. 2011 [cit. 2012-04-03]. Dostupné z: http://www.vexcor.cz/saas/sla/.

(SMEJKAL, 2010) SMEJKAL, Vladimír; RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 3., roz. a aktualiz. vydání. Praha : Grada, 2010. 354 s. ISBN 978-80-247-3051-6.

(SNEDAKER, 2007) SNEDAKER, Susan. *Business Continuity and Disaster Recovery Planning for IT Professionals*. United States of America: SYNGRESS, 2007. ISBN 978-1-59749-172-3.

(STONEBURNER, 2002) STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis. *Risk management guide for Information Technology Systems* [online]. Gaithersburg : NIST Special Publication 800-30, 2002 [cit. 2011-10-24]. Dostupné z WWW: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

(TECHTARGET, 2008-2012) Enterprise disaster recovery planning guide. TECHTARGET. *SearchDisasterRecovery* [online]. copyright © 2008-2012 [cit. 2012-02-22]. Dostupné z: http://searchdisasterrecovery.techtarget.com/.

Seznam zkratek

ALE - Annualized Loss Expectancy

BC/DR - Business continuity/Disaster Recovery

BCM - Business Continuity Management

BCP - Business Continuity Planning

BIA - Business Impact Analysis

CCTA - Central Computer and Telecommunications Agency

CRAMM - CCTA Risk Analysis and Management Method

ČSN - Česká Státní norma

DB - Data Base

DIR - Directory (file systems)

DoS - Denial of Service

DRP - Disaster Recovery Plan

ERP - Enterprise Resource Planning

FTP - File Transport Protocol

HW - Hardware

ICT - Information and Communication Technologies

IN - Input

ISO/IEC - International Organization for Standardization/International Electrotechnical Commission

IT - Information Technology

IT PM - IT Project Management

ITIL - IT Infrastructure Library

ITSM - IT Service Management

LAN - Local Area Network

MTV - Maximálně tolerovatelný výpadek

OUT - Output

PC - Personal Computer

PDCA - Plan-Do-Check-Act

POP3 - Post Office Protocol

RA - Risk assessment

SDLC - System Development Lifecycle

SLA - Service Level Agreement

SMTP - Simple Mail Transfer Protocol

Seznam pojmů

Akceptovatelné riziko – schopnost organizace akceptovat určitou úroveň rizika.

Analýza dopadů (Business Impact Analysis) – jedná se o klíčový prvek pro řízení kontinuity činností organizace. Analyzují se zde procesy organizace a dopady při jejich přerušení na fungování jednotlivých služeb v organizaci. Obvykle obsahuje také kvalitní zhodnocení dopadu formou finančního vyčíslení ztrát, snížení úrovně poskytovaných služeb nebo kvalitativní posouzení dopadu. V procesu BIA se určí mimo dopadu také minimální úroveň zdrojů, které jsou potřebné k obnovení procesů firmy.

Audit – jde o úřední přezkoumání a zhodnocení dokumentů nezávislou osobou. Účelem je zde zjistit kvalitu vnitřního fungování firmy. Máme finanční audity, audity dopadů na životní prostředí a v našem kontextu by se měl provést audit našeho návrhu na obnovu služeb, tedy DRP plánu.

Brainstorming – je skupinová technika zaměřená na generování co nejvíce nápadů na dané téma. Je založena na skupinovém výkonu.

Buffer – značí vyrovnávací paměť, která je určena pro dočasné uchování dat před jejich přesunem na místo jiné.

Byznys incident tým (Business incident team) – tento tým řeší chyby, výpadky a navrhuje nápravná opatření podle jejich charakteru.

Byznys (Business) – je to činnost organizace, která vyrábí výrobky nebo poskytuje služby svým zákazníkům.

Cíl obnovy činnosti (Recovery Point Objective) – určuje akceptovatelnou úroveň množství dat, která budou po havárii obnovena. Tím bude zajištěno, že pro každou z definovaných aktivit nebude ztraceno více dat, než definuje maximální tolerovatelná ztráta dat (Maximum Tolerable Data Loss).

CRAMM - Pro potřeby vlády Velké Británie. Dnes je široce využíván jako prostředek pro analýzu rizik v případech, kdy je vyžadován souhlas s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799. Analýza CRAMM řeší ohodnocení systémových aktiv, dále seskupení aktiv do logických skupin a stanovení hrozeb, které působí na tyto skupiny, prozkoumání zranitelnosti systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny. Poté jsou navrhnuta bezpečnostní opatření, která jsou vymezena ve shodě s úrovní rizika při porovnání s již implementovanými systémovými opatřeními.

Doba obnovy činností (Recovery Time Objective) – určuje akceptovatelný čas od obnovení funkčnosti, který zaručuje, že maximální interval výpadku pro každou z definovaných činností ve firmě není překročen.

Dopad (Impact) – pomocí ekonomických nebo neekonomických ukazatelů vyjádřím důsledek působení hrozby.

ERP (Enterprise resource planning) – je informační systém, který integruje a automatizuje velké množství procesů souvisejících s produkční činností podniku. Jde většinou o výrobu, logistiku, distribuci a další.

Incident – neočekávaná nebo neobvyklá událost bez specifikace rozsahu, která může způsobit přerušení činností v organizaci.

ITIL (Information Technology Infrastructure Library) – jedná se o dokumentovaný rámec, který popisuje nejlepší způsoby řízení a správy IT služeb v organizaci. Zabývá se také zlepšováním a měřením kvality dodávaných služeb IT a to nejen z pohledu firmy ale také našeho zákazníka. Knihovny ITIL jsou také východiskem mezinárodních norem ČSN ISO/IEC 20000.

Kontinuita činností organizace (Business Continuity) – zajišťuje strategické a taktické schopnosti organizace plánovat a reagovat na vzniklé incidenty, zachovávat či v určitém čase na předem určené úrovni obnovit svou činnost.

Krizová událost – jedná se o událost, která způsobí přerušení nebo i havárii, pokud není správně řízena a tím zvládnuta. Neřízené a nezvládnuté kritické události mají silný negativní vliv na činnost, pověst, hodnotu a hlavně celkové přežití organizace.

Log – je název pro záznam, které si programy vytvářejí pro ukládání informací o své činnosti a běhu. Slouží ke zpětné analýze a k rozpoznání, zda došlo k nějaké chybě a pokud ano, pomáhají určit, k jaké chybě došlo a z jakého důvodu.

Maximální přijatelná ztráta údajů (Maximum tolerable data loss) – maximálně přijatelný objem ztráty dat v průběhu havárie, aniž by došlo k ohrožení nebo závažnému dopadu na procesy v organizaci.

Maximální přijatelný interval výpadku (Maximum tolerable outage) – maximální časový interval nedostupnosti procesů a činností, ve kterém pravděpodobně dojde i k ohroožení spojitosti činnosti organizace.

Metodika CRAMM – vytvořena pro potřeby vlády Velké Británie. Dnes je široce využíván jako prostředek pro analýzu rizik v případech, kdy je vyžadován souhlas s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799. Analýza CRAMM řeší ohodnocení systémových aktiv, dále seskupení aktiv do logických skupin a stanovení hrozeb, které působí na tyto skupiny, prozkoumání zranitelnosti systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny.

Plán kontinuity činností (Business Continuity Plan) – jde o zdokumentování procedur a informací, které mají být připraveny a udržovaný pro použití v případu incidentu, tak aby organizace byla schopna pokračovat v činnosti na přijatelné úrovni.

Plán obnovy (Disaster recovery) – jedná se o havarijní plán, dokumentaci zdrojů, činností a úkolů při obnově technických prostředků a infrastruktury v případě havárie. Vzhledem k systému řízení kontinuity činností je plán obnovy jeho podmnožinou.

Plán zvládnutí incidentů (Incident management plan) – je to plán činností, které jsou prováděny v případě vzniku nepříznivé události, tedy incidentu. Obsahuje seznam klíčových zaměstnanců, zdrojů, služeb a aktivit, které jsou součástí procesu zvládnutí incidentu.

Pohroma – je neočekávaná události velkého rozsahu, která může způsobit havárii nebo kompletní přerušení činnosti organizace.

POP3 (Post Office Protocol) – je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta.

Proces – jde o označení pro postupné a nějak zaměřené děje nebo změny, pro posloupnost stavů nějakého systému. Průběh procesu, který můžeme předvídat, lze označit jako proces zákonitý. V opačném případě jde o proces nahodilý (stochastický).

Riziko – vše, co má nějaký vliv na činnosti v organizaci a může je nějak negativně ohrozit

Řízení kontinuity činností (Business continuity management) – je řídící proces, který identifikuje potencionální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu procesů v organizaci v předem stanovené minimální úrovni, v případě narušení nebo ztráty.

Řízení rizik (Risk management) – jde o činnost, která se zaměřuje na identifikaci, analýzu a ohodnocení rizik a přípravu jejich zvládnutí.

Služba – je hospodářská činnost, která uspokojuje určitou potřebu. Výsledkem služby je užitečný efekt.

SMTP (Simple mail transfer protocol) – je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů).

Strategie obnovy (Recovery strategy) – zde určíme záložní způsoby, díky kterým je možné obnovit činnost organizace na požadovanou úroveň v případě vzniku incidentu.

Zhodnocení rizika (Risk Assessment) – nám pomůže s identifikací, analýzou a ohodnocením rizik.

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 25. 4. 2012

Michaela Funková

.....

jméno a příjmení studenta

Seznam obrázků a tabulek

Obrázky:

Tabulky:

Seznam příloh

Příloha č. 1:	Formulář s časovými rozvrhy jednotlivých fází při tvorbě plánu obnovy
Příloha č. 2:	Formulář s kontaktními informacemi na členy krizového týmu
Příloha č. 3:	Formulář s kontaktními informacemi na externí firmy
Příloha č. 4:	Formulář Business Impact Analysis nekritických služeb firmy